ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΑΘΗΜΑΤΙΚΟ ΕΦΑΡΜΟΓΩΝ – ΑΝΑΛΥΣΗ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗ

Bitcoin, πλατφόρμα Blockchain και ECDSA

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΝΑΓΙΩΤΗ Β. ΚΟΝΤΟΓΙΑΝΝΗ

Επιβλέπουσα :Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιανουάριος 2018

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας πτυχιακής εργασίας, θέλουμε να ευχαριστήσουμε για την καθοδήγηση και επίβλεψη την κυρία Θ.Βαρβαρίγου, καθηγήτρια της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών.

ΑΝΑΣΚΟΠΙΣΗ

Η παρούσα εργασία πραγματεύεται το κρυπτονόμισμα Bitcoin, την πλατφόρμα λειτουργίας του, Blockchain και τον αλγόριθμο(ECDSA) που χρησιμοποιείται για την ασφαλή επικοινωνία των χρηστών με την παραγωγή και διαχείριση μηνυμάτων και κλειδιών.
Παρουσιάζουμε τον κίνδυνο παραβίασης του blockchain υπό καθεστώς επίθεσης διπλής δαπάνης (double spent attack) καθώς και τον κίνδυνο παραβίασης και αλλοίωσης, (ECDSA), των μηνυμάτων από την χρήση μη ασφαλών ελλειπτικών καμπυλών υπό καθεστώς μοντελοποιημένων επιθέσεων.

Blockchain
Είναι ένας συνεχώς αυξανόμενος κατάλογος αρχείων, που ονομάζονται blocks, τα οποία συνδέονται και ασφαλίζονται με κρυπτογραφία. Κάθε block τυπικά περιέχει έναν δείκτη κατακερματισμού ως σύνδεσμο προς ένα προηγούμενο block, ένα χρονικό σήμα και δεδομένα συναλλαγής.

Digital Signatures
Αποτελούν ένα μαθηματικό σχήμα, που χρησιμοποιείται καθημερινά για την έγκριση ψηφιακών εγγράφων και μηνυμάτων παντός είδους στο χώρο τις κρυπτογραφίας.

Double Spend Attack
Οι επιθέσεις διπλής δαπάνης αποτελούν έναν από τους πιθανούς τρόπους παραβίασης της πλατφόρμας του Bitcoin και γενικότερα του συστήματος των κρυπτονομισμάτων, όπου το ίδιο ποσό που μεταφράζεται σε αντίστοιχο ψηφιακό σήμα δαπανάται δύο ή και περισσότερες φορές κυρίως μέσω της αντιγραφής ή πλαστογράφησης του.

ECDSA
Μαθηματικός κρυπτογραφικός αλγόριθμος που χρησιμοποιείται στην ασφαλή παραγωγή και διαχείριση της πληροφορίας της υπογραφής.

Μαθηματικό υπόβαθρο αλγορίθμου ECDSA και δομικά στοιχεία αυτού.

- Ελλειπτικές Καμπύλες
- Πεδία Galois
- Διασυνδεσιμότητα – διαδραστικότητα ελλειπτικών καμπυλών και πεδίων Galois

Εφαρμογή και Αποτελέσματα χρήσεως ECDSA
Ο αλγόριθμος παράγει ζεύγη κλειδιών ιδιωτικών και δημοσίων τα οποία συνοδεύουν τα αποστελόμενα μηνύματα με σκοπό την διασφάλιση της αυθεντικότητας και μοναδικότητας των μηνυμάτων.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ ΣΤΟ BITCOIN

Το Κρυπτονόμισμα είναι μία peer-to-peer αποκεντρωμένη ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών. Τα περισσότερα κρυπτονομίσματα κάνουν χρήση μιας Κατανεμημένης Βάσης Δεδομένων ως πυλώνα του συστήματος τους, το Blockchain.

Το bitcoin που παρουσιάστηκε το 2009, έγινε το πρώτο επιτυχημένο αποκεντρωμένο κρυπτονόμισμα. Λόγω της ανοικτής φύσης του λογισμικού του, επετράπη σε πολλούς προγραμματιστές να πειραματιστούν με τον κώδικά του και να τον τροποποιήσουν (forking). Δημιουργήθηκε κατά αυτόν τον τρόπο ένα πλήθος νέων κρυπτονομισμάτων στα οποία έχουν γίνει προσπάθειες για να βελτιωθούν ή και να προστεθούν λειτουργικότητες όπως ταχύτερες συναλλαγές και μεγαλύτερη ανωνυμία.

Το κυριότερο χαρακτηριστικό του κρυπτονομίσματος είναι ο αποκεντρωτικός χαρακτήρας του και μέσω αυτού η ανθεκτικότητά του σε κάθε μορφής προσπάθεια για έλεγχο και παρέμβαση.

Σύμφωνα με αναλυτές η Αμερικάνικη κρίση της περιόδου του 2008 που οδήγησε σε τρώση του τραπεζικού συστήματος και αμφισβήτηση των παραδοσιακών δομών διαχείρισης του χρήματος, ήταν η αφορμή για την επινόηση του.

Όπως οι κυβερνήσεις προστατεύουν την οικονομία των χωρών τους από κάθε είδους εγκληματική ενέργεια και αστάθεια, μέσα από συνεχή έλεγχο και χρηματοοικονομικά εργαλεία, παρομοίως τα κρυπτονομίσματα διατηρούνται ασφαλή μέσα από την χρήση της κρυπτογραφίας προκυμμένου να αποτρέπονται κακόβουλες ενέργειες(hacking), αλλά και εσωτερικές παραβιάσεις που θα οδηγούσαν την πλατφόρμα σε αστάθεια και θα ανάγκαζαν τους χρήστες να ξαναγυρίσουν στις παραδοσιακές διατραπεζικές λύσεις.

Το Bitcoin στηρίζει την λειτουργία του σε φαινομενικά απλά και γνωστά εργαλεία, κάνοντας έτσι την απόπειρα δημιουργίας ενός καινούργιου κρυπτονομίσματος από εξοικειωμένους χρήστες δυνατή.

Η τεχνολογία πάνω στην όποια δομήθηκε το Bitcoin είναι εκείνη του Blockchain,

Blockchain είναι ένας συνεχώς αυξανόμενος κατάλογος αρχείων, που ονομάζονται blocks, τα οποία συνδέονται και ασφαλίζονται με κρυπτογραφία. Κάθε block περιέχει έναν δείκτη κατακερματισμού ως σύνδεσμο προς ένα προηγούμενο block, ένα χρονικό σήμα και δεδομένα συναλλαγής. Με το σχεδιασμό, οι block αλυσίδες είναι ανθεκτικές στην τροποποίηση των δεδομένων. Καθένα από τα blocks περιέχει ένα δείκτη κατακερματισμού(hash pointer) που το συνδέει με το προηγούμενο και ένα χρονικό σήμα. Ο τρόπος αποθήκευσης των πληροφοριών χαρακτηρίζεται από μονιμότητα και η επαλήθευση του περιεχομένου του είναι απλή. Άπαξ και αναρτηθεί ένα block οποιαδήποτε τροποποίηση σε αυτό ή σε κάποιο από τα προηγούμενα, δεν μπορεί να είναι αναδρομική, χωρίς αλλαγή και σε όλα τα προηγούμενα, στοιχείο το οποίο κάνει τον κατάλογο αυτό συμπαγή.Η θεωρία πίσω από την ανάρτηση των blocks του παραπάνω

καταλόγου είναι γνωστή και ως hashing (κατακερματισμός). Οι συναρτήσεις κατακερματισμού, γνωστότερες ως hash functions περιγράφονται στο επόμενο κεφάλαιο.

Κεφάλαιο 1 Δομικά στοιχεία του Bitcoin

1.1 Η κρυπτογραφική μέθοδος του κατακερματισμού (hashing)

Η συνάρτηση κατακερματισμού(hash function) έχει αξιωματική υπόσταση με την μαθηματική έννοια του όρου, για την επιστήμη της κρυπτογραφίας. Λαμβάνοντας σαν όρισμα ένα οποιουδήποτε μεγέθους μήνυμα χορδή (string), το οποίο αποτελείται από γράμματα, αριθμούς και σύμβολα, η ίδια η συνάρτηση μέσα από τον μαθηματικό της τύπο το μετασχηματίζει-χαρτογραφεί σε ένα αντίστοιχο string.

Η λειτουργία κατακερματισμού επίσης επιτρέπει σε κάποιον να επαληθεύσει εύκολα για το αν το μήνυμα εισόδου αντιστοιχεί σε δεδομένη τιμή κατακερματισμού θεωρώντας τα δεδομένα εξόδου γνωστά. Στη περίπτωση που δεν γνωρίζω ή δεν μπορώ να ανακτήσω τα αρχικά μου μηνύματα, είναι εξαιρετικά δύσκολο να ανακτηθεί το αρχικό περιεχόμενο του μηνύματος γνωρίζοντας την αποθηκευμένη τιμή κατακερματισμού (hash value).

Η ανωτέρω λειτουργία χρησιμοποιείται συστηματικά για τη διασφάλιση της ακεραιότητας των μεταδιδόμενων δεδομένων και αποτελεί το δομικό στοιχείο για την παροχή ελέγχου ταυτότητας μηνυμάτων.

Θεμελιώδη χαρακτηριστικά της συνάρτησης κατακερματισμού είναι:

1. **Αντοχή στις συγκρούσεις(collision resistance):** έννοια σύμφωνα με την οποία μια συνάρτηση κατακερματισμού F είναι ανθεκτική σε συγκρούσεις τιμών εισόδου εάν είναι αρκετό δύσκολο αν όχι αδύνατο να οδηγηθούμε σε κοινή τιμή έξοδού από διαφορετικά ορίσματα. Αλλιώς για x, y με $x \neq y$ να καταλήξω στο $F(x) = F(y)$.

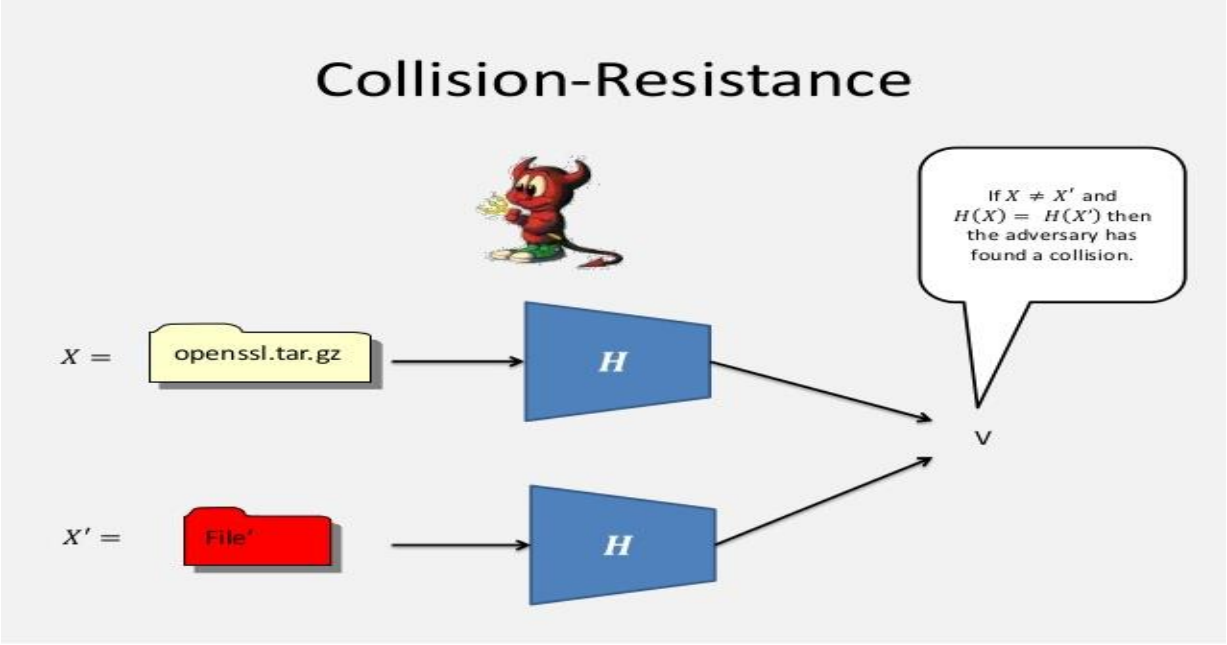


Figure 1.1: Γραφική απεικόνιση μιας hash function H, που παρουσιάζει σύγκρουση τιμών εξόδου.

Βέβαια καμία τέτοια συνάρτηση δεν μπορεί να κατασκευαστεί, από την στιγμή που μια συνάρτηση κατακερματισμού με περισσότερες εισόδους από τις εξόδους θα παρουσιάσει αναγκαστικά συγκρούσεις.

Η αντοχή στις συγκρούσεις (collision resistance) αφορά τις συναρτήσεις για τις όποιες συγκρούσεις δύσκολα προκύπτουν.

Ίσως η πιο γνωστή hash function, που χρησιμοποιείται και στο Bitcoin, είναι η SHA-256 που παράγει 256 bits εξόδου από ένα αυθαίρετα μεγάλου μεγέθους string. Σύμφωνα με την αρχή του περιστερώνα συγκρούσεις αναμφίβολα θα προκύψουν.

Αρχή του περιστερώνα (floor function): Για φυσικούς αριθμούς r και n, αν $u = r \cdot n + 1$ αντικείμενα κατανέμονται σε n σύνολα, τότε η αρχή του περιστερώνα υποστηρίζει ότι τουλάχιστον ένα από τα σύνολα θα περιέχει τουλάχιστον $r + 1$ αντικείμενα. Για αυθαίρετους u και n αυτό γενικεύεται στο $r + 1 = \{(u - 1) / n\} + 1$.

Εφαρμογή - Message digest

Μια πολύ πρακτική εφαρμογή της συνάρτησης κατακερματισμού είναι η επαλήθευση του περιεχομένου ενός προσωπικού φακέλου, αρχείου ή μηνύματος. Συγκεκριμένα χρησιμοποιώντας ως μήνυμα εισόδου το παραπάνω (προσωπικό φάκελο, αρχείο ή μήνυμα) στην συνάρτηση κατακερματισμού και λαμβάνοντας ως έξοδο το 256bits hash μπορούμε να ελέγξουμε ανά πάσα στιγμή την αυθεντικότητα του επαληθεύοντας απλά το hash.

Δίνεται έτσι η δυνατότητα στο χρήστη να αποφύγει την αποθήκευση μεγάλων αρχείων και να προστατεύσει το περιεχόμενο από οποιαδήποτε απόπειρα αλλαγής συγκρίνοντας τα hashes.

Η αντοχή στις συγκρούσεις συνεπάγεται την δεύτερη αντοχή προβλέψεων, όχι όμως και την πρώτη.

2. **Πρώτη Αντοχή προβλέψεων(preimage resistance*):*** για προκαθορισμένη τιμή εξόδου y, είναι υπολογιστικά ανέφικτη η εύρεση της τιμής εισόδου x που την έχει ως έξοδο, δηλ. είναι δύσκολο να βρεθεί οποιαδήποτε προεπιλογή x, έτσι ώστε $F(x) = y$.

   Δεύτερη Αντοχή προβλέψεων(second preimage resistance*):* είναι ανέφικτο για διαφορετική τιμή είσοδού x', με $x' \neq x$, να ισχύει $F(x) = F(x')$.

Θέλοντας να δώσουμε μια πιο σαφή εικόνα για την αντίσταση των συγκρούσεων και την δυσκολία να βρεθεί μια τέτοια σύγκρουση στην SHA-256 όπου αναμένεται string με μέγεθος εξόδου 256 bits, από την θεωρία πιθανοτήτων θα χρειαζόταν $\mathbf{2^{130} + 1 < \nu < 2^{256} + 1}$ διαφορετικές τιμές εισόδου. Υπολογίζοντας τα αντίστοιχα hashing results, θα προέκυπτε η πρώτη σύγκρουση με πιθανότητα 99.8%. Ένας απλός υπολογιστής με ικανότητα να υπολογίσει 10.000 hashes ανά δευτερόλεπτο, θα χρειαστεί περισσότερο από ένα 10^{27} χρόνια για να το πράξει.

3. **Δυνατότητα Απόκριψης(Hiding):** μια συνάρτηση κατακερματισμού έχει την δυνατότα να αποκρυβεί εάν για μια κρυφή τιμή i, η οποία επιλέγεται από μια κατανομή με υψηλή min-entropy, για δεδομένη τιμή $F(i \parallel z)$ είναι αδύνατον να βρεθεί η τιμή z.

Η συγκεκριμένη ιδιότητα μας επιβεβαιώνει ότι για συγκεκριμένη τιμή y = F(x), όπου x η άγνωστη τιμή εισόδου και y η γνωστή τιμή εξόδου αντίστοιχα, είναι πρακτικά αδύνατον με κάποιο τρόπο να καταλάβω ποια είναι η τιμή εισόδου. Ουσιαστικά το x, πρέπει να επιλεγεί από ένα σύνολο θεωρητικά πολύ μεγάλο. Άρα λοιπόν, εάν πράγματι επιλέξουμε αρκετά πολλά διαφορετικά x από ένα τέτοιου τύπου σύνολο, θα καταλήξουμε στο συμπέρασμα ότι είναι εξαιρετικά απίθανο να καταλήξω στην αρχική τιμή y.

Στη περίπτωση του SHA-256, επιλέγοντας τυχαία ένα από τα string εξόδου μεγέθους 256bits, η πιθανότητα να επιλέγαμε το πολύ συγκεκριμένο θα ήταν $\frac{1}{2^{256}}$, πιθανότητα εξαιρετικά μικρή.

Εφαρμογή- Commitment Scheme: Μια εφαρμογή της παραπάνω ιδιότητας, η οποία είναι γνωστότερη ως διαδικασία δέσμευσης, ξεκινά χρησιμοποιώντας – δεσμεύοντας μια πολύ συγκεκριμένη τιμή(message) και εκδίδοντας ένα δεσμευτικό συμβόλαιο. Εάν θελήσουμε να αποκαλύψουμε το περιεχόμενο του συμβολαίου, δημιουργούμε ένα κλειδί(key) και μια τιμή εξόδου.

Χρησιμοποιώντας την συνάρτηση SHA-256 παράγουμε το κλειδί του δεσμευτικού συμβολαίου. Σε συνέχεια με τη βοήθεια της ανωτέρω συναρτήσεως προβαίνουμε σε hashing του κλειδιού και του μηνύματος παράγοντας έτσι το δεσμευτικό συμβόλαιο. Εάν κάποιος θελήσει να επαληθεύσει την διαδικασία, θα πρέπει να κάνει hashing στο ζεύγος του κλειδιού-μηνύματος και να ελέγχει εάν το πρώτο hashing είναι ίδιο με το αντίστοιχο του ζεύγους.

Σκοπός του όλου εγχειρήματος(του πολλαπλού hashing) είναι η απόδειξη της δεσμευτικής ιδιότητας. Εάν η συνάρτηση κατακερματισμού είναι ανθεκτική σε σύγκρουση (collision resistant), τότε θα είναι ανέφικτη η εύρεση διακριτών τιμών msg_1 και msg_2 έτσι ώστε να ισχύει F (key ‖ msg_1) = F (key ‖ msg_2). Άρα θα ισχύουν και οι προαναφερθείσες ιδιότητες της απόκρυψης και της δεσμευτικότητας .

Βασικά στοιχεία διαδικασίας δέσμευσης

- **(com):=commit(msg,key)**: όπου με την συγκεκριμένη εντολή έχοντας ως είσοδο την αρχική τιμή και το κλειδί της δέσμευσης, προκύπτει το δεσμευτικό συμβόλαιο.
- **IsValid:=verify(com,msg,key)**: η συγκεκριμένη εντολή λαμβάνοντας ως είσοδο το δεσμευτικό συμβόλαιο, το κλειδί του και το μήνυμα, μας επιστρέφει True εάν επαληθεύεται το περιεχόμενο. Σε αντίθετη περίπτωση επιστρέφει την λογική τιμή False.
- **Δυνατότητα απόκρυψης**: για δεδομένο συμβόλαιο, είναι αδύνατη η ανάκτηση του μηνύματος που αποκρύψαμε.
- **Δεσμευτικότητά**: είναι αδύνατον το ίδιο κλειδί για την δέσμευση ενός συμβολαίου, να μας δόσει ένα δεύτερο συμβόλαιο διαφορετικό του αρχικού, δηλάδη verify((msg,key),key,msg2)==true.

4. **Γνώρισμασμα του γρίφου(puzzle friendliness):** Μια συνάρτηση κατακερματισμού μπορεί να χαρακτηριστεί ως προς τον τρόπο αντιμετώπισης της ως γρίφος, εάν για μια y τιμή εξόδου μεγέθους n-bits επιλέγοντας ένα φυσικό αριθμό w από μια κατανομή με υψηλή εντροπία ελαχίστου(high min entropy), ο χρόνος εύρεσης της τιμής εισόδου x από τον τύπο $F(w \mid\mid x) = y$ είναι πρακτικά αδύνατον να είναι μικρότερος από 2^n δευτερόλεπτα.

Εάν κάποιος χρήστης θελήσει από την αρχική λειτουργία κατακερματισμού να καταλήξει σε μία συγκεκριμένη τιμή εξόδου y, όπου η τιμή εισόδου x επιλέγεται έστω και τμηματικά με τυχαίο τρόπο, τότε είναι πολύ δύσκολο να καταλήξει στην y, με αρχική τιμή έστω $x^* \neq x$, δηλαδή σε σύγκρουση.

(Θεωρητικό Παράρτημα): Στο σημείο αυτό παρατίθεται η θεωρία Εντροπίας Ελαχίστου (min Entropy Theory)

Γνωρίζουμε από την θεωρία πιθανοτήτων, ότι η εντροπία του ελαχίστου (min) ενός διακριτού τυχαίου συμβάντος x με πιθανές καταστάσεις $1,2,\dots,N$, όπου N φυσικός αριθμός και με αντίστοιχες πιθανότητες $p_1, p_2, \dots, p_N$, είναι:

$$H_\infty = \min_i{}^n(-\log(p_i)) = -\max_i(\log(p_i)) = -\log(\max_i(p_i)$$

Η βάση του λογαρίθμου είναι απλώς μια σταθερά κλιμάκωσης. Στα υπολογιστικά συστήματα, τα οποία χρησιμοποιούν το δυαδικό σύστημα, η βάση του λογαρίθμου είναι 2, δηλαδή $\log_2()$. Οπότε μια κατανομή χαρακτηρίζεται από εντροπία ελαχίστου με τουλάχιστον b ψηφία (bits), αν καμία από τις πιθανές καταστάσεις δεν έχει πιθανότητα μεγαλύτερη από $2 - b$.

Ο συμβολισμός $H_\infty(X)$ προκύπτει από την παραμετρική οικογένεια των μέτρων εντροπίας τύπου Shannon. Επιπλέον η εντροπία Rényi, της οποίας ο τύπος είναι:

$$H_k(X) = -\log^{k-1}\sqrt{\sum_i (p_i)^k}$$

Καθώς το k αυξάνεται, δίνεται το μεγαλύτερο βάρος στις μεγαλύτερες πιθανότητες και οριακά καθώς το $k \to \infty$ μόνο η μεγαλύτερη πιθανότητα p_i έχει κάποια επίδραση στο τελικό αποτέλεσμα.

Εφαρμογή – Γρίφος(Puzzle): Είναι ένα πολύπλοκο μαθηματικό πρόβλημα το οποίο προϋποθέτει η λύση να ανήκει σε ένα πολύ μεγάλο σύνολο πιθανών τιμών χωρίς να υπάρχουν έμμεσες συντομότερες λύσεις. Επιθυμούμε ο γρίφος να είναι δύσκολος στην επίλυση του.

Τα δομικά στοιχεία γρίφου:

- Η λύση ενός γρίφου είναι η τιμή εισόδου x, που επαληθεύει τον τύπο $F(code||x)$ και ανήκει σε σύνολο τιμών Y, όπου F είναι η συνάρτηση κατακερματισμού, ενώ το code είναι αποτελεί την τιμή ταυτοποίησης του γρίφου.
- Το code επιλέγεται από μια κατανομή υψηλής εντροπίας ελαχίστου, πράγμα που σημαίνει ότι δεν υπάρχουν άλλες συντομότερες λύσεις του παραπάνω προβλήματος. Επιλέγεται από τυχαία γεννήτρια (code generator function).

Για τιμή εξόδου n-bits, η τιμή x μπορεί να πάρει 2^n διαφορετικές τιμές. Το μέγεθος του συνόλου Y καθορίζει την δυσκολία του γρίφου και συνήθως είναι αρκετά μικρότερο από το πεδίο ορισμού των τιμών x.

Συνάρτηση συμπίεσης μονής κατεύθυνσης(one-way compression function)

Συνάρτηση συμπίεσης μονής κατεύθυνσης, είναι μια συνάρτηση που μετατρέπει αναμιγνύοντας δύο εισόδους σταθερού μήκους σε έξοδο σταθερού μήκους. Ο μετασχηματισμός είναι μη αναστρέψιμος, πράγμα που σημαίνει ότι είναι δύσκολο δεδομένης μιας συγκεκριμένης εξόδου να υπολογιστούν οι εισροές που συμπιέζονται σε αυτή την έξοδο.

Η ανάμιξη γίνεται με τέτοιο τρόπο ώστε κάθε bit εξόδου να εξαρτάται από κάθε bit εισόδου, γνωστότερο και ως φαινόμενο χιονοστιβάδας.

1.1 The Merkle–Damgård construction

Εξίσου σημαντικό εργαλείο της κρυπτογραφίας είναι η κατασκευή μιας Merkle–Damgård συνάρτησης κατακερματισμού. Είναι μια μέθοδος κατασκευής κρυπτογραφικών συναρτήσεων κατακερματισμού ανθεκτικών σε συγκρούσεις τιμών από συναρτήσεις συμπίεσης μονής κατεύθυνσης, το είδος των οποίων χρησιμοποιείται κατά κόρων στη σχεδίαση αλγορίθμων κατακερματισμού όπως ο γνωστός SHA-256, στον οποίο το Bitcoin στηρίζεται.

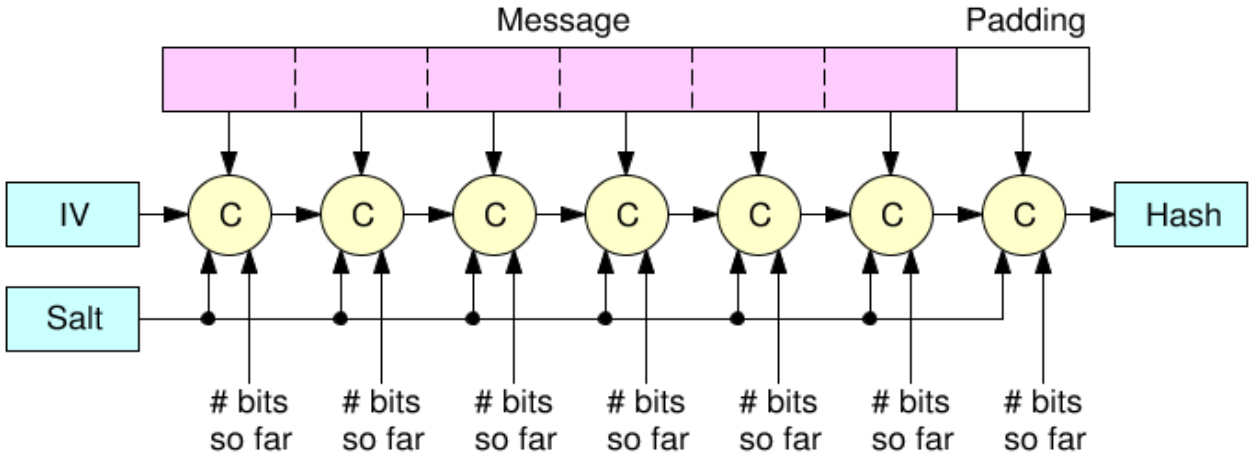


Figure 1.2.1: Μία τυπική αναπαράσταση ενός Merkle–Damgård αλγορίθμου

- Ο αλγόριθμος αρχίζει με μια αρχική τιμή, τον φορέα αρχικοποίησης (IV).
- Για κάθε block μηνύματος, η συνάρτηση συμπίεσης (ή συμπύκνωσης) C λαμβάνει ως είσοδο το παρόν αποτέλεσμα, το συνδυάζει με το block-μήνυμα και παράγει ένα ενδιάμεσο αποτέλεσμα. Η διαδικασία επαναλαμβάνεται παρόμοια.
- Στο τελευταίο block προστίθενται μηδενικά όπως απαιτείται προκυμμένου το σύνολο των ψηφίων να αντιπροσωπεύει το μήκος ολόκληρου του μηνύματος.

Στη προσπάθεια να δυσκολέψουμε περισσότερο την παραπάνω διαδικασία κατακερματισμού, συχνά χρησιμοποιούμε μια συνάρτηση οριστικοποίησης (finalisation function). Πολλές φορές αποτελεί μια παραλλαγή της συνάρτησης συμπίεσης (ή συμπύκνωσης) C, ενώ ο ρόλος της ποικίλει. Η συμπίεση μιας μεγαλύτερης εσωτερικής κατάστασης σε μικρότερο μέγεθος κατακερματισμού εξόδου ή η εξασφάλιση καλύτερης ανάμειξης στα δυαδικά ψηφία του ποσού κατακερματισμού συχνά καλύπτουν το γενικότερο σκοπό.

Έχει αποδειχθεί ότι αν η συνάρτηση συμπίεσης μονής κατεύθυνσης C είναι ανθεκτική σε συγκρούσεις τότε θα είναι επίσης ανθεκτική και η τελική συνάρτηση κατακερματισμού που θα κατασκευάσουμε.

Δυστυχώς όμως η όλη διαδικασία παρουσιάζει προβλήματα και αδυναμίες. Συγκεκριμένα προσπάθειες εύρεσης των hashing results είναι ευκολότερες σε μεγάλου μήκους μηνύματα, τεχνική πιο αποτελεσματική από την κατακλυσμιαία δοκιμή υποψήφιων τιμών εισόδου.

1.3 Hash pointers, Blockchains και Merkle Trees

Hash Pointer

Ο δείκτης κατακερματισμού, γνωστότερος και ως hash pointer, αποτελεί την βασική δομή κατασκευής δομών αποθήκευσης και διαχείρισης πληροφοριών, όπως το blockchain, στην επιστήμη της κρυπτογραφίας. Σε τέτοιου είδους δομές αποθηκεύουμε μέρος πληροφορίας, μαζί με το αποτέλεσμα της συνάρτησης κατακερματισμού που προκύπτει δίνοντας ως είσοδο την πληροφορία αυτή. Βασικό πλεονέκτημα της δομής είναι η δυνατότητα προστασίας και επαλήθευσης της πληροφορίας από πιθανές κακόβουλες αλλαγές στο περιεχόμενο(hacking).

Σε ατομικό επίπεδο η χρησιμότητα του είναι μηδαμινή, όμως ο συνδυασμός τους οδηγεί σε χρήσιμες εφαρμογές.

Blockchain

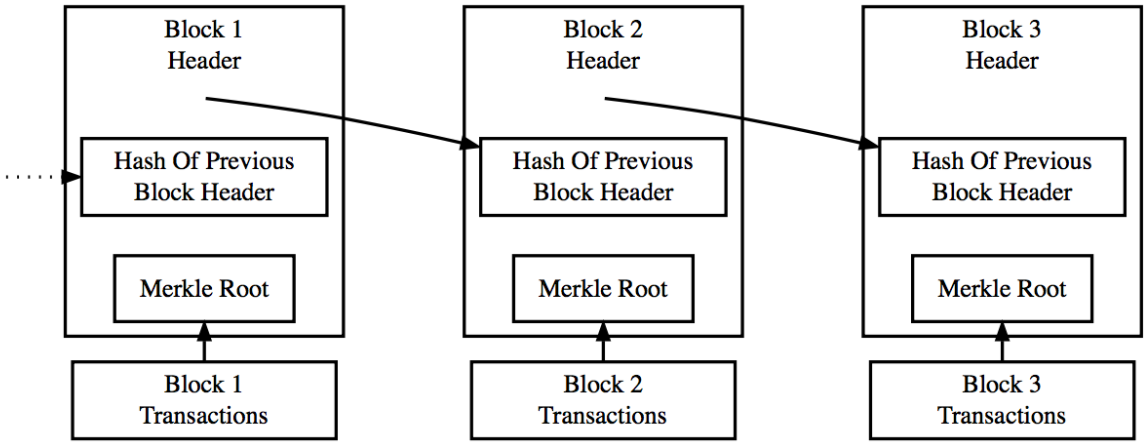
Το blockchain αποτελεί μια κατανεμημένη βάση δεδομένων σειράς αρχείων ή σύστημα πληροφόρησης και λειτουργεί ως ημερολόγιο όλων των συναλλαγών ή των ψηφιακών γεγονότων που έχουν εκτελεστεί και μοιραστεί μεταξύ των συμμετεχόντων μερών της ομάδας εργασίας. Βασικό πλεονέκτημα της τεχνολογίας είναι η ανοχή σε βλάβες, κακόβουλες επιθέσεις και αλλοιώσεις. Τα παραπάνω καθιστούν την τεχνολογία δυνητικά κατάλληλη για την καταγραφή γεγονότων, οικονομικών και ιατρικών αρχείων και δραστηριοτήτων επί αυτών όπως η διαχείριση ταυτοτήτων και τεκμηρίωση προέλευσης φαρμακευτικών προϊόντων, επεξεργασία συναλλαγών και ανασκόπηση τους.

Βασικό χαρακτηριστικό του blockchain είναι ότι κάθε είδους συναλλαγή που καταγράφεται επαληθεύεται με τη συναίνεση της πλειοψηφίας των συμμετεχόντων στο σύστημα και από την στιγμή εκείνη και μετά δεν διαγράφεται ποτέ. Η ίδια η εφαρμογή περιέχει επαληθευμένες πληροφορίες σχετικά με οποιαδήποτε συναλλαγή πραγματοποιήθηκε πότε στο blockchain.

Κατά αυτό τον τρόπο, έφερε μια νέα τάξη πραγμάτων στο χώρο της μέχρι τότε κεντροποιημένης ψηφιακής οικονομίας με την εισαγωγή της ελεύθερης σε πρόσβαση αυτοδιαχειριζόμενης βάσης των δεδομένων.

Το Bitcoin, παρόλο που θεωρείται αμφιλεγόμενο ως ψηφιακό νόμισμα και είναι το πλέον αποκεντροποιημένο δίκτυο ομότιμων χρηστών, είναι ίσως το σαφέστερο παράδειγμα της τεχνολογίας οι εφαρμογές της οποίας συναντώνται σχεδόν σε όλες τις επιστήμες.

Από τεχνολογικής απόψεως το blockchain είναι μια σειριακή απεικόνιση από δείκτες κατακερματισμού. Η απεικόνιση αυτή αναφορικά με το περιεχόμενο της είναι εξηρτημένη από το προηγούμενο block. Κάθε block έχει κάποια βασικά χαρακτηριστικά, τα οποία είναι:



Simplified Bitcoin Block Chain

- Η κεφαλή του block(Block Header): Η κεφαλή περιλαμβάνει έναν αριθμό αναφοράς του block μοναδικό στο είδος του, μια χρονική ένδειξη και έναν σύνδεσμο πίσω στο προηγούμενο block, ο οποίος είναι το hashing της κεφαλής του προηγούμενου block.
- Η ρίζα του δέντρου Merkle(Merkle root): η ρίζα του δέντρου που περιλαμβάνει το συγκεκριμένο block.
- Περιεχόμενο των συναλλαγών(Content of transactions): Περιλαμβάνεται επίσης, το ποσό της συναλλαγής και τις διαδικτυακές διευθύνσεις εκείνων που συμμετείχαν στη συναλλαγή.

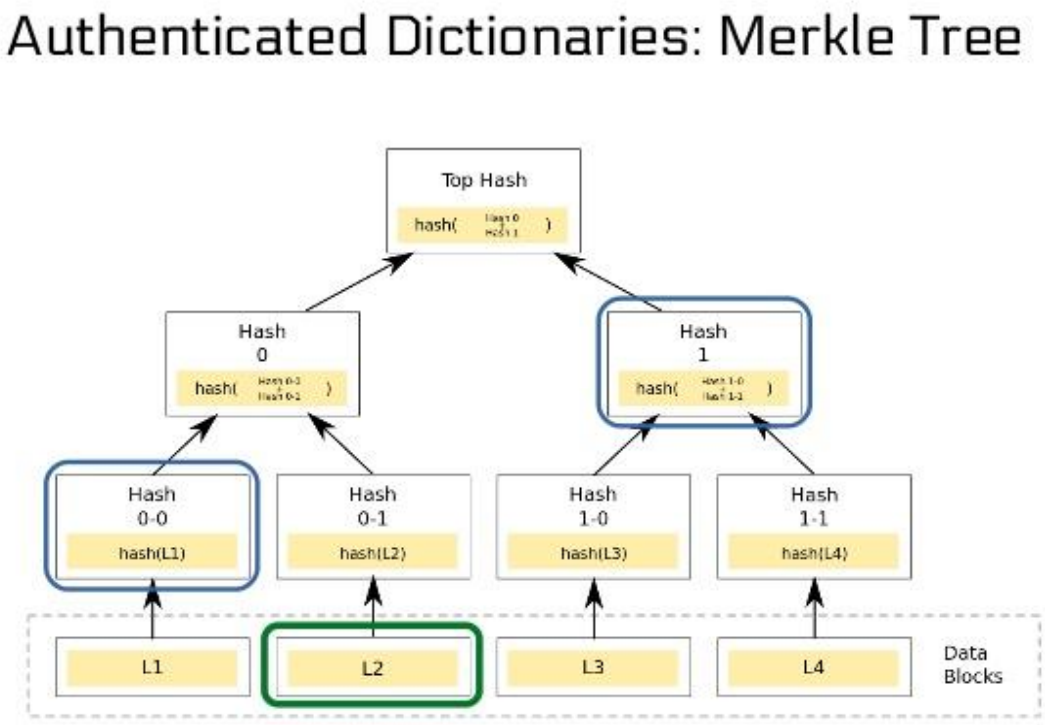
Η ασφάλεια που προσφέρει η δομή της αλυσίδας εξηγείται από το γεγονός ότι εάν κάποιος χρήστης θελήσει να παραβιάσει την αλυσίδα αλλοιώνοντας το περιεχόμενο οποιουδήποτε block, θα πρέπει να καλύψει αυτή την τροποποίηση αλλάζοντας και το hash του προηγούμενου block. Φυσικά μπορεί να συνεχίσει να κάνει αυτό, αλλά η στρατηγική θα αποτύχει όταν φτάσει στο κεφάλι της λίστας, λόγω του ότι είναι αδύνατον να αλλάξεις όλες τις κεφαλές κατακερματισμού μέχρι την αρχή του blockchain. Μια τέτοια προσπάθεια θα γινόταν άμεσα αντιληπτή από την κοινότητα, από την στιγμή που δεν θα κατάφερνε να διατηρήσει την συνέπεια της.

Merkle Tree

Ίσως η χρησιμότερη από όλες τις προηγούμενες δομές στην επιστήμη της κρυπτογραφίας είναι το δέντρο κατακερματισμού γνωστότερο και ως Merkle tree, στο οποίο κάθε κόμβος – φύλλο, φέρει ως κεφαλή το αποτέλεσμα της συνάρτησης κατακερματισμού με τιμή εισόδου τις κεφαλές όλων των υπο-κόμβων του. Η διαδικασία αυτή τερματίζει στη ρίζα του δέντρου, η οποία εννοιολογικά περιέχει τμήματα από τα hashαρίσματα όλων των υπο-κόμβων.

Το πρόβλημα της χρονικής σήμανσης, γνωστότερο ως timestamping λύθηκε χάρις τα δέντρα κατακερματισμού. Συγκεκριμένα θέλοντας να διαπιστωθεί αν ένα ή περισσότερα έγγραφα

δημιουργήθηκαν μια δεδομένη στιγμή, δρομολογείται μια σειρά από συναλλαγές που περιλαμβάνουν τις πληροφορίες των εγγράφων.



Το μεγαλύτερο πλεονέκτημα του δέντρου των hashes είναι η αποτελεσματική και ασφαλής αποθήκευση τεράστιων δομών δεδομένων και άλλων αρχείων. Η ανασκόπηση της πληροφορίας είναι πολύ εύκολη διότι το μόνο που απαιτείται από τον χρήστη είναι να θυμάται την τιμή της κεφαλής του δείκτη κατακερματισμού, δηλαδή την hash value. Οποιαδήποτε παραποίηση του περιεχομένου, όπως και πριν γίνεται άμεσα αντιληπτή από την στιγμή που οι δείκτες κατακερματισμού θα έχουν διαφορετική τιμή για τον συγκεκριμένο δείκτη, αλλά και για την ρίζα του ίδιου του δέντρου. Άρα αρκεί κανείς να θυμάται την κεφαλή της ρίζας για να μπορεί με σιγουριά να ισχυριστεί ότι η πληροφορία παραμένει ανέπαφη.

Για να ελέγξουμε εάν ένας δείκτης κατακερματισμού ανήκει ή όχι σε ένα δέντρο είναι απαραίτητο να ελέγξουμε ολόκληρο το δέντρο; Την απάντηση στο ερώτημα αυτό δίνει η ακόλουθη εφαρμογή.

Εφαρμογή του Merkle Δέντρου

Έλεγχος ιδιότητας Μέλους

Σε αντίθεση με το blockchain, σε ένα Merkle δέντρο είναι εφικτή η απόδειξη ότι ορισμένα δεδομένα ανήκουν σε δείκτη κατακερματισμού, ο οποίος με την σειρά του ανήκει στο δέντρο. Ουσιαστικά ελέγχουμε την ιδιότητα μέλους του δείκτη στο όλο δέντρο, γνωρίζοντας όπως και πριν μόνο την κεφαλή του δείκτη.

Αρκεί να ελέγξουμε τα block ξεκινώντας από την ρίζα μέχρι το συγκεκριμένο block που περιέχει την πολύτιμη πληροφορία, ελέγχοντας τις κεφαλές κατά τον γνωστό τρόπο. Ο χρόνος που απαιτείται για να γίνει ο παραπάνω έλεγχος είναι υπολογίσιμος.

Συγκεκριμένα για N κόμβους δέντρου, απαιτείται κατά μέσο όρο $Log(N)$ δευτερόλεπτα. Όποτε και για ένα πολύ μεγάλο δέντρο, ο χρόνος ελέγχου είναι σχετικά μικρός.

Έλεγχος ιδιότητας Μη-Μέλους

Με όμοιο τρόπο μπορούμε να ελέγξουμε ότι η πληροφορία ενός κόμβου κατακερματισμού δεν ανήκει στο δέντρο, αποδεικνύοντας ότι εν λόγο κόμβος δεν ανήκει σε αυτό. Στους ενδιάμεσους κόμβους η κεφαλή κατακερματισμού αποτελεί το συγκεντρωτικό hashing των κεφαλών των υποκόμβων του. Άρα συγκρίνοντας την κεφαλή του κόμβου με το hashing που έχουμε ως δεδομένο αντιλαμβανόμαστε άμεσα για τον αν ο υποκόμβος ανήκει ή όχι.

Παρατήρηση: Εξαρχής ο έλεγχος είναι εφικτός λόγο της σειριακής παρουσίασης και αποθήκευσης της πληροφορίας. Εάν παρουσιάζονταν διακλαδώσεις στο δέντρο της βάσεως δεδομένων κατά το μονοπάτι του ελέγχου θα εγκλωβιζόμασταν σε κύκλο, οπότε δεν θα καταλήγαμε ποτέ στον επιθυμητό κόμβο για να συγκρίνουμε τα αποτελέσματα της συνάρτησης κατακερματισμού.

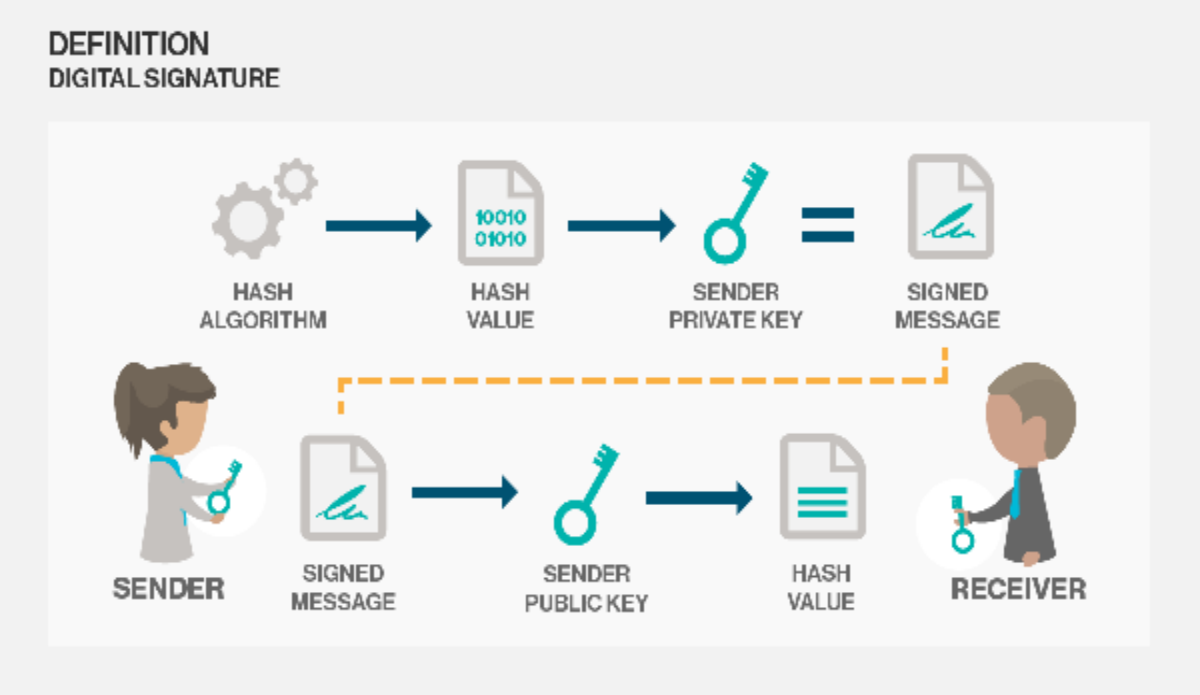
1.4 Ψηφιακές Υπογραφές (Digital Signatures)

Οι ψηφιακές υπογραφές, αποτελούν μία μαθηματική εφαρμογή, που χρησιμοποιείται καθημερινά για την έγκριση ψηφιακών εγγράφων και μηνυμάτων παντός είδους στο χώρο της κρυπτογραφίας. Αποτελούν το ψηφιακό ανάλογο μιας χειρόγραφης υπογραφής που λαμβάνει χώρα κατά την επικύρωση ενός συμβολαίου ή άλλων πειστήριων από τις συμμετέχουσες πλευρές με παρόμοιες ιδιότητες και ίδια βαρύτητα.

Είναι ένα τυπικό στοιχείο των περισσότερων κρυπτογραφικών πρωτοκόλλων και χρησιμοποιείται μαζικά στη διανομή λογισμικού, τις χρηματοοικονομικές συναλλαγές, το λογισμικό διαχείρισης συμβολαίων, αλλά και σε όσες άλλες εφαρμογές εγκυμονούν κίνδυνο πλαστογραφίας ή αλλοίωσης του περιεχομένου.

Σε γενικές γραμμές επιθυμούμε μια ψηφιακή υπογραφή να χαρακτηρίζεται από εγκυρότητα και μοναδικότητα. Οποιοσδήποτε αρμόδιος να μπορεί να επιβεβαιώσει την αυθεντικότητα της ο δε αποστολέας του μηνύματος δεν μπορεί μετά την προσθήκη της ψηφιακής υπογραφής να αρνηθεί είτε την αποστολή του μηνύματος είτε το αναλλοίωτο αυτού. Εκάστη ψηφιακή υπογραφή είναι μονοσήμαντα συνδεδεμένη με το εκάστοτε μήνυμα, αρχείο ή έγγραφο, ώστε να μην μπορεί να επαναληφθεί η χρήση της για την υπογραφή οποιουδήποτε άλλου. Ιδιότητα που στην πραγματικότητα διασφαλίζει ότι κανένας δεν μπορεί να αποκόψει την υπογραφή από το ίδιο το έγγραφο και να την επικολλήσει σε κάποιο άλλο.

Κρυπτογραφικά η ψηφιακή υπογραφή χρησιμοποιείται, όπως στο παρακάτω σχεδιάγραμμα:



Αναπαράσταση της διαδικασίας αποστολής – λήψης ψηφιακά υπογεγραμμένων αρχείων και συναλλαγών.

Η βασική μορφή των εντολών σε επίπεδο ψευδοκώδικα για τη δημιουργία, υπογραφή και επικύρωση ενός κρυπτοσυβολαίου είναι:

- **(sk, pk) := generateKeys(keysize, 1^k)** : με την οποία έχοντας στο νου μας το μέγεθος του κλειδιού παράγουμε το ζεύγος του κρυφού(secret key) και του δημοσίου κλειδιού(public key). Το πρώτο χρησιμοποιείται για την υπογραφή των αρχείων και προτείνεται να φυλάσσεται σε ασφαλές σημείο, σε περίπτωσή που απαιτείται η ανάκτηση του. Το τελευταίο, γίνεται γνωστό σε όλα τα μέλη της κοινότητας, ώστε να μπορούν να επαληθεύσουν την ιδιοκτησία της εκάστοτε υπογραφής. Η ποσότητα k αποτελεί μία παράμετρο ασφαλείας.
- **Sig: = sign (sk,mesg):** όπου έχοντας ως είσοδο το μήνυμα-αρχείο και το κρυφό κλειδί, λαμβάνουμε ως έξοδο μια υπογραφή για το υπογεγραμμένο πλέον μήνυμα.

- **isValid := verify(pk,mesg,sig):** η οποία μας επιστρέφει true, εάν η υπογραφή sig επιβεβαιώνει ότι το υπογεγραμμένο μήνυμα-αρχείο έχει υπογραφεί από το συγκεκριμένο δημόσιο κλειδί, έχοντας ως τιμές εισόδου το δημόσιο κλειδί, το αρχείο και τη παραπάνω υπογραφή. Σε αντίθετη περίπτωση επιστρέφει την τιμή false.

Παρατηρήσεις: Οι παραπάνω εντολές generate, sign πρακτικά είναι αλγόριθμοι κατασκευής τυχαίων τιμών για μεγαλύτερη ασφάλεια και μαζική παραγωγή τέτοιων κλειδιών σε αντίθεση με την verify της οποίας το αποτέλεσμα είναι καθοριστικό για την όλη διαδικασία.

Οι ψηφιακές υπογραφές πρέπει να είναι αναγκαίες και ικανές, πράγμα που σημαίνει ότι χωρίς γνώση του μυστικού κλειδιού sk που αντιστοιχεί στο δημόσιο κλειδί pk, κανένας κακόβουλος χρήστης - αντίπαλος δεν μπορεί με οιοδήποτε τρόπο να παράξει ζεύγος μηνυμάτων υπογραφής (sig, mesg), όπου verify (pk, sig, mesg) = true

Παραδείγματα κλειδιών για την πραγματοποίηση μιας συναλλαγής.

1.4.1 Συστήματα παραγωγής ψηφιακών κλειδιών(Key Generation Algorithms)

Τα σύγχρονα κρυπτογραφικά συστήματα περιλαμβάνουν αλγόριθμους συμμετρικού κλειδιού (όπως DES και AES) και αλγόριθμους δημόσιου κλειδιού (όπως το RSA). Οι πρώτοι χρησιμοποιούν μόνο ένα κλειδί σε όλες τις διαδικασίες, πράγμα που καθιστά την διαφύλαξη του προτεραιότητα. Οι δημόσιου κλειδιού χρησιμοποιούν ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού. Το δημόσιο κλειδί είναι διαθέσιμο στη κοινότητα και εκδίδεται συνήθως μέσω ψηφιακού πιστοποιητικού. Ο εκάστοτε αποστολέας κρυπτογραφεί τα δεδομένα με το δημόσιο κλειδί, τα οποία μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει.

Στη προσπάθεια να αποφευχθούν τα μειονεκτήματα, προκυμμένου να αξιοποιηθούν στο μέγιστο δυνατό βαθμό οι παραπάνω τεχνικές, τα σύγχρονα συστήματα όπως το TLS και SSH χρησιμοποιούν ένα συνδυασμό των δύο: το ένα μέρος λαμβάνει το δημόσιο κλειδί του άλλου και κρυπτογραφεί ένα μικρό κομμάτι δεδομένων (είτε ένα συμμετρικό κλειδί ή μερικά δεδομένα που χρησιμοποιήθηκαν για την παραγωγή του). Το υπόλοιπο της συνομιλίας χρησιμοποιεί έναν (συνήθως πιο γρήγορο) αλγόριθμο συμμετρικού κλειδιού για την κρυπτογράφηση.

Γενικότερα στη κρυπτογραφία, χρησιμοποιούνται ακέραιοι για κλειδιά, που παράγονται από γεννήτριες τυχαίων αριθμών(RNG) ή ψευδοτυχαίων αριθμών(PRNG). Εναλλακτικά τα κλειδιά παράγονται κατά τρόπο αιτιοκρατικό, μέσα από την χρήση φράσεων πρόσβασης ή συναρτήσεων εξαγωγής κλειδιών. Για ακόμα καλύτερα αποτελέσματα σε επίπεδο ασφάλειας χρησιμοποιούνται ποικίλες άλλες μέθοδοι. Βέβαια πολλά σύγχρονα πρωτόκολλα έχουν σχεδιαστεί να δημιουργούν καινούργια δημόσια κοινόχρηστα κλειδιά σε κάθε συναλλαγή.

Χαρακτηριστικά των μηχανισμών παραγωγής ψηφιακών κλειδιών είναι:

- **Τυχαιότητα(Randomness):** Οι μηχανισμοί πρέπει να παράγουν τυχαία αποτελέσματα, καθώς η έλλειψη του τυχαίου δημιουργεί θέματα ασφαλείας.
- **Μέγεθος Μηνύματος-Αρχείου:** σε κάθε τέτοια δομή, υπάρχει σταθερό όριο στο μέγεθος των αρχείων/μηνυμάτων που μπορεί να κανείς να υπογράψει, από την στιγμή που ο υπολογιστής μεταφράζει το περιεχόμενο σε bits & bytes. Το πρόβλημα λύνεται εάν αντί για το μήνυμα υπογραφθεί μόνο το αποτέλεσμα κατακερματισμού(hash) του περιεχομένου, διότι κατά αυτό τον τρόπο επικυρώνουμε την 256 bit τιμή εξόδου της οποίας το μέγεθος είναι σταθερό και μπορεί να αφορά ένα αρχείου υπερπολλαπλασίου μεγέθους. Επιπλέον, έχουμε αναφέρει ότι οι συναρτήσεις κατακερματισμού είναι ανθεκτικές σε συγκρούσεις, οπότε το τέχνασμα είναι ασφαλές.

1.4.2 Υποδομές Δημοσίων Κλειδιών (PKIs)

Οι υποδομές δημοσίων κλειδιών επιτρέπουν στους χρήστες ενός συστήματος να βρουν και να επαληθεύσουν τα δημόσια κλειδιά βάση ταυτοτήτων άλλων χρηστών. Είναι υπεύθυνες για την ευκολότερη διανομή και πιστοποίηση δημοσίων κλειδιών και διατηρούν μεγάλες βάσεις δεδομένων για τα γνωστά ζεύγη (id,pk). Στοχεύουν στην ακριβή καταχώρηση που συνεπάγεται την αδυναμία ενός χρήστη να καταχωρήσει και να διατηρήσει ταυτότητα που δεν του ανήκει, δηλαδή να μιμηθεί μια υπάρχουσα στο σύστημα ταυτότητα.

Οι μέχρι τώρα προσεγγίσεις πάνω στις υποδομές παρουσιάζουν προβλήματα, λόγω της έλλειψης επαρκούς ασφάλειας. Οι βασικές λειτουργίες των PKIs είναι:

- Καταχώρηση των ζευγών ταυτοτήτων και δημοσίων κλειδιών.

- Ενημέρωση του δημόσιου κλειδιού που αντιστοιχεί σε προηγούμενη ταυτότητα, σε περιπτώσεις που απαιτείται ή ο χρήστης το επιθυμεί.
- Αναζήτηση ενός δημόσιου κλειδιού που αντιστοιχεί σε υπάρχουσα στη βάση δεδομένων ταυτότητα.
- Επαλήθευση ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί στην αντίστοιχη καταχωρημένη ταυτότητα, με τρόπο πιο αποτελεσματικό από την απλή αναζήτηση.
- Ανάκληση του δημόσιου κλειδιού που αντιστοιχεί στη ταυτότητα του ζεύγους.

Μπορεί κανείς να υποστηρίξει ότι η διατήρηση ταυτότητας είναι το πιο ουσιαστικό στοιχείο ασφάλειας. Χρησιμοποιούνται για όλους τους παραπάνω στόχους δύο ειδών δομές, οι Αρχές Πιστοποίησης, γνωστότερα ως CAs, καθώς και τα αποκεντρωμένα δίκτυα πιστοποίησης ομότιμων χρηστών ή αλλιώς Webs of Trust.

CAs: Οι CAs ενεργούν ως αξιόπιστος φορέας υπεύθυνος για τη διανομή και τη διαχείριση ψηφιακών πιστοποιητικών για όλο το δίκτυο. Στη πράξη η χρήση αυτών δημιουργεί περιορισμένα σημεία αποτυχίας στην υποδομή δημοσίων κλειδιών, κυρίως λόγο της υπερβολικής εμπιστοσύνης από μέρος του δικτύου. Περιστατικά, όπως παραβίαση(hacking) των φορέων που οδηγούν σε εσφαλμένα πιστοποιητικά δεν είναι λίγα. Επιπλέον παρά την κεντροποιημένη διαχείριση δεν εξασφαλίζεται η συνέπεια, δεδομένου ότι υπάρχουν πολλαπλές CAs που μπορούν να πιστοποιούν διαφορετικά δημόσια κλειδιά που αντιστοιχούν στην ίδια ταυτότητα, παραβιάζοντας έτσι τη διατήρηση της ταυτότητας(identity retention).

Εναλλακτική Αντιμετώπιση: Στη προσπάθεια να εισάγουμε περισσότερη διαφάνεια, στις λειτουργίες των CAs, προτείνεται η διατήρηση δημόσιων αρχείων καταγραφής μόνο για συγκεκριμένο αριθμό ανεξάρτητων εξυπηρετητών παγκοσμίως και κάθε τέτοιος διακομιστής καταγραφής μπορεί να εκτελείται από ξεχωριστή CA. Στη συνέχεια, τα καταγεγραμμένα αρχεία θα ελέγχονται για την αποφυγή ύποπτων βεβαιώσεων από άλλους εξυπηρετικούς μηχανισμούς(servers), καθώς και για τη συνεπή συμπεριφορά από ελαφρύ λογισμικό ελεγκτών το οποίο μπορεί να εκτελεστεί από οποιονδήποτε. Αυτό θα εξασφαλίσει ότι ο ιδιοκτήτης μιας διεύθυνσης διαδικτύου(ip) θα μπορεί να δει όλα τα πιστοποιητικά που εκδόθηκαν για την διεύθυνση του και έτσι θα είναι σε θέση να εντοπίσει τυχόν λανθασμένα πιστοποιητικά, διασφαλίζοντας τη διατήρηση της ταυτότητας.

Webs of Trust: τα οποία λειτουργούν τελείως διαφορετικά από τα παραπάνω. Σε αυτό το σύστημα, ο έλεγχος ταυτότητας είναι απολύτως αποκεντρωμένος από την στιγμή που από τους χρήστες δημιουργείται ένα πιστοποιητικό που περιλαμβάνει τις συσσωρευμένες υπογραφές τους επί της αξιοπιστίας των νέων δημοσίων κλειδιών και τέλος το ίδιο το κλειδί. Αυτό το σύστημα επωφελείται από την κατανεμημένη του φύση επειδή απομακρύνει οποιοδήποτε σημείο αποτυχίας. Δυστυχώς, όμως δεν υπάρχει εγγύηση συνέπειας και τίποτα δεν εμποδίζει πολλούς χρήστες να δημιουργούν δημόσια κλειδιά για την ίδια ταυτότητα, **άρα δεν ικανοποιείται η προϋπόθεση της διατήρησης της ταυτότητας.**

1.5 Τα μαθηματικά της Διαδικασίας Εξόρυξης (Mining)

Όπως έχει προαναφερθεί η πλατφόρμα του Bitcoin, προκυμμένου να διατηρήσει την ισορροπία μεταξύ της ικανότητας εξόρυξης και του αριθμού των block που επικυρώνονται από τους ανθρακωρύχους, ελέγχει αυξομειώνοντας την δυσκολία των hashes. Οι ίδιοι προσπαθούν να υπολογίσουν τα αποτελέσματα κατακερματισμού μέσω των επιθέσεων δύναμης (force attack) με χρήση υπολογιστικών συστημάτων. Συχνά στον αγώνα της εξόρυξης συμμετέχουν κακόβουλοι χρήστες, οι οποίοι προσπαθούν να επιτεθούν στην πλατφόρμα. Μία από τις επιθέσεις είναι εκείνη της διπλής δαπάνης η οποία μελετήθηκε από τους δημιουργούς του Bitcoin.

Αρχικά βάση πρωτοκόλλου συμβολίζουμε, ως εξής:

- Ο ενδιάμεσος χρόνος για την δημιουργία ενός block, συμβολίζεται με T, ενώ στη περίπτωση του k-ου block ο ενδιάμεσος χρόνος θα είναι T_k.
- $\tau_0 = E[T] \coloneqq 600s$, δηλαδή 10 λεπτά.
- t, τον χρόνο που χρειάστηκε για να εξορισθούν τα τελευταία 2016 blocks.
- α, συμβολίζεται η παράμετρος της εκθετικής κατανομής της T, που εκφράζει την ταχύτητα εξόρυξης.
- $N(t)$, ο αριθμός των block που έχουν επικυρωθεί μέχρι την χρονική στιγμή t. Προφανώς αρχικά έχω $t = 0$.
- p, q, με $q \in \left(0, \frac{1}{2}\right) \kappa\alpha\iota\ p = 1 - q$, την ικανότητα κατακερματισμού(hash power), μιας ομάδας κακόβουλων χρηστών και μιας ομάδας ανθρακωρύχων αντίστοιχα.

Σημείωση: Για να ξεχωρίζουμε τα ποσά που αφορούν τους ανθρακωρύχους, από τα αντίστοιχα που αναφέρονται στους επίδοξους hackers, γράφουμε τα δεύτερα τονούμενα.

Για κάθε επόμενο επίπεδο δυσκολίας hashing, ο απαιτούμενος χρόνος υπολογίζεται σε:

$$T_{trgnew} = T_{trgold} * \frac{t}{2016\tau_0}$$

Γενικά το hashing κάθε επόμενου block-κόμβου ξεκινά από την αρχή, οπότε για μεταβλητή χρόνου T, με χρονικά διαστήματα $t_1, t_2 > 0$ θα ισχύει:

$$P(T > t_1 + t_2 | T > t_2) = P[T > t_1],$$

Οπότε, σε επόμενο βήμα:

$$P[T > t_1 + t_2] = P[T > t_1 + t_2 | T > t_2] * P[T > t_2] = P[T > t_1] * P[T > t_2]$$

Η παραπάνω εξίσωση και το όρισμα συνέχειας υποδηλώνουν ότι ο χρόνος T είναι μια εκθετικά κατανεμημένη τυχαία μεταβλητή, δηλαδή:

$$f_T(t) = ae^{-at}$$

όπου για $\alpha = \frac{1}{600}\sec^{-1}$.

Από τα παραπάνω οι ενδιάμεσοι χρόνοι μεταξύ των εξορύξεων $T_1, T_2, \dots, T_n$, που είναι ανεξάρτητες ομοιόμορφα κατανεμημένες τυχαίες μεταβλητές ακολουθούν προφανώς την εκθετική κατανομή $f_T(t)$.

Ο συνολικός χρόνος $S_n = T_1 + T_2 + \cdots + T_n$, ακολουθεί βάσει του πίνακα αθροιστικών κατανομών τυχαίων μεταβλητών:

$$f_{S_n}(t) = \frac{a^n}{(n-1)!} t^{n-1} e^{-at}$$

Που δεν είναι άλλη από την κατανομή Γαμμα με παραμέτρους (n, a), ενώ η σωρευτική κατανομή είναι:

$$F_{Sn}(t) = \int_0^t f_{Sn}(u)du = 1 - e^{-at} \sum_{k=0}^{n-1} \frac{(at)^k}{k!}$$

Για $S_0 = 0$, παίρνω το διάστημα $N(t) = \{k \geq 1; S_k \leq t\} = \max\{n \geq 0; S_n < t\}$. Η τυχαία μεταβλητή $N(t)$ ακολουθεί την κατανομή Poisson με παράμετρο αt, όπου:

$$P[N(t) = k] = \frac{(at)^k}{k!} e^{-at}$$

Άρα από την στιγμή που θα έχω $N(t) = n$, που ισοδυναμεί με $S_n \leq t \; και \; S_{n+1} > t$ θα έχω:

$$P[N(t) = n] = F_{Sn}(t) - F_{Sn+1}(t) = \frac{(at)^n}{k!} \, e^{-at} \, .$$

<u>Λήμμα 1</u>: Θεωρούμε q_n, την πιθανότητα ενός συμβάντος E_n να προκύψει μετά από την επικύρωση n πλοκ. Για την πιθανότητα q_n, ισχύει:

$$q_n = \left(\frac{q}{p}\right)^n$$

<u>(Απόδειξη)</u>: Για $q_0 = 1 \;\; q_1 = \frac{q}{p}$, από την ιδιότητα των Μαρκοβιανών αλυσίδων θα ισχύει:

$$q_{n+m} = P[E_{n+m}] = P[E_n|E_m] \cdot P[E_m] = P[E_n] \cdot P[E_m] = q_n \cdot q_m$$

Επιπλέον ισχύει η ιδιότητα του τυχαίου περιπάτου από την στιγμή που μιλάμε για ανεξάρτητα μεταξύ τους συμβάντα, η οποία είναι:

$q_n = qq_{n-1} + pq_{n+1}$, όπου λόγω $q_0 = 1$ & $q_n \to 0$, θα ισχύει $q_n = \left(\frac{q}{p}\right)^n$.

Από την στιγμή που οι T, T' είναι ανεξάρτητες τυχαίες μεταβλητές μεταξύ τους και ακολουθούν αντίστοιχες κατανομές θα έχω

$$p = P[T < T'] = \frac{a}{a + a'}\ , \text{οπότε λόγω } q = 1 - p \text{ έχω } q = 1 - \frac{a}{a + a'} = \frac{a'}{a + a'}.$$

Επιπλέον το $\inf(T, T')$, ακολουθεί την εκθετική κατανομή με παράμετρο $a + a'$ που αντιπροσωπεύει την συνολική ικανότητα εξόρυξης των ομάδων των επιτιθέμενων και των ανθρακωρύχων μαζί. Στο Bitcoin $a + a' = \tau_0 = 600\ sec$. Άρα ισχύουν:

$$E[T] = \frac{1}{\alpha} = \frac{\tau_0}{p} \ \ \kappa\alpha\iota\ E[T'] = \frac{1}{a'} = \frac{\tau_0}{q}.$$

Συνεχίζοντας, θεωρώντας h, h' τις ικανότητες κατακερματισμού των ανθρακωρύχων και των επιτιθέμενων αντίστοιχα, για $h + h'$, την συνολική ικανότητα και των δύο ομάδων μαζί, ισχύον τα εξής:

$$p = \frac{h}{h + h'}\ \kappa\alpha\iota\ q = 1 - p = \frac{h'}{h + h'}$$

Τώρα για t_0, t_0' το μέσο χρονικό διάστημα που χρειάζεται για να επικυρώσουν το επόμενο block οι ανθρακωρύχοι και οι επιτιθέμενοι αντίστοιχα:

$(h + h')\tau_0 = m, ht_0 = m$ & $h't_0' = m$, υπολογίζουμε το χρόνο τ_0:

$\tau_0 = \frac{t_0 t_0'}{t_0 + t_0'}$, όπως επίσης

$$p = \frac{t_0'}{t_0 + t_0'} = \frac{\tau_0}{t_0} \ \ \&\ \ q = \frac{t_0}{t_0 + t_0'} = \frac{\tau_0}{t_0'}$$

Από όλα τα παραπάνω μπορούμε πλέον να συνδέσουμε τις πιθανότητες p, q με τις α, α' ικανότητες εξόρυξης, ως εξής:

$$p = \frac{a}{a + a'}\ \kappa\alpha\iota\ q = \frac{a}{a + a'}$$

ΚΕΦΑΛΑΙΟ 2 Επίθεση κατά του Blockchain

Επιθέσεις διπλής δαπάνης στο Bitcoin

Εισαγωγή

Οι επιθέσεις διπλής δαπάνης αποτελούν έναν από τους πιθανούς τρόπους παραβίασης της πλατφόρμας του Bitcoin και γενικότερα του συστήματος των κρυπτονομισμάτων, όπου το ίδιο ποσό που μεταφράζεται σε αντίστοιχο ψηφιακό σήμα δαπανάται δύο ή και περισσότερες φορές κυρίως μέσω της αντιγραφής ή πλαστογράφησης του.

Είναι φαινόμενα που οδηγούν σε πληθωρισμό, εξαιτίας της εμφάνισης περισσότερων νομισμάτων που δεν αναγνωρίζει άμεσα η πλατφόρμα και υποτίμησης του νομίσματος σε σχέση με άλλα κρυπτονομόσματα. Η εμπιστοσύνη των καταναλωτών κλονίζεται, ενώ η κυκλοφορία του επηρεάζεται σε μεγάλο βαθμό. Οι θεμελιώδεις κρυπτογραφικές τεχνικές για την αποτροπή διπλών δαπανών διατηρώντας ταυτόχρονα την ανωνυμία των συμμετεχόντων σε μια συναλλαγή είναι το σύστημα των ψηφιακών υπογραφών.

Οι αρχικές προβλέψεις των πολέμιων της πλατφόρμας του Bitcoin έδειχναν ότι η απουσία μιας κεντρικής δομής ελέγχου και επαλήθευσης των συναλλαγών θα οδηγούσε με μαθηματική ακρίβεια στην κατάρρευση του κρυπτονομίσματος. Όμως οι δημιουργοί του Bitcoin, στηριζόμενοι στη δομή του ψηφιακού νομίσματος με την χρήση ψηφιακών υπογραφών, στη ομοφωνία και κοινή συναίνεση των χρηστών της αλυσίδας του Blockchain και στην απόδειξη εργασίας που προσφέρουν οι ανθρακωρύχοι(miners) έδειξαν ότι μέχρι στιγμής η πλατφόρμα έχει περιορίσει επιτυχώς το κίνητρο για προσπάθεια διενέργειας διπλών δαπανών, καθιστώντας δημόσιες τις πληροφορίες σχετικά με το ιστορικό συναλλαγών του και δυσκολεύοντας τους επίδοξους hackers. Ο κίνδυνος όμως είναι υπαρκτός και ιστορικά επιβεβαιωμένος.

2.1 Μαθηματικό υπόβαθρο επιθέσεων διπλής δαπάνης

Αρχικά θεωρούμε:

- q ∈ (0, ½), την πιθανότητα που αντιπροσωπεύει την ικανότητα κατακερματισμού(hash power), μιας ομάδας κακόβουλων χρηστών
- p=1-q, την αντίστοιχη των ανθρακωρύχων.

Γνωρίζουμε επίσης τις εξής κατανομές:

1. $\Gamma(x) := \int_0^{+\infty} t^{x-1}e^{-t}dt$, $όπου\ x > 0$, κατανομή Γάμμα(Gamma function).
2. $B_x(a,b) := \int_0^x t^{a-1}(1-t)^{b-1}dt, όπου\ x \in [0,1]$, $με\ a,b > 0\ για\ a,b \in R$, κατανομή Βήτα(Bêta function). Συνήθως το $x = 1$ και τότε ισχύει $B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$
3. Την κανονικοποιημένη μορφή της παραπάνω κατανομής , όπου $I_\chi(a,b) := \frac{B_x(a,b)}{B(a,b)}$

Θεώρημα: Μετά την επικύρωση του z^ου block από τους miners, η πιθανότητα για $s = 4pq$ μια επίθεση διπλής δαπάνης να επιτύχει είναι:

$$P(z) = I_{4pq}\left(z, \frac{1}{2}\right), \text{ όπου}$$

$$I_x(a,b) = \frac{B_x(a,b)}{B(a,b)} = \frac{1}{\frac{\Gamma(\alpha)\Gamma(b)}{\Gamma(\alpha+b)}} B_x(a,b), \text{ οπότε θα έχω:}$$

$I_x(a,b) \coloneqq \frac{\Gamma(\alpha+b)}{\Gamma(\alpha)\Gamma(b)} \int_0^x t^{a-1}(1-t)^{b-1} dt$, είναι η ρυθμιζόμενη ελλιπής μορφής συνάρτηση B (beta function).

(Απόδειξη):

Αποδεικνύεται ότι η σωρευτική συνάρτηση κατανομής μιας αρνητικής δυαδικής τυχαίας μεταβλητής x, είναι:

$$F_x(k) = \Pr[X \le k] = \sum_{l=0}^{k} p^z q^l \binom{l+z-1}{l} = 1 - I_p(k+1, z), \textit{ όπου:}$$

$$I_p(k,z) - I_p(k+1,z) = \frac{p^k q^k}{kB(k,z)}, \text{ ώστε να ισχύει } P(z) = 1 - I_p(z,z) + I_q(z,z)$$

Επιπλέον από την σχέση συμμετρίας της συνάρτησης Βήτα, ισχύει:

$$I_p(a,b) + I_q(b,a) = 1,$$

στη συνέχεια θέτοντας $t \to 1 - t$ στη σχέση, προκύπτει:

$$I_p(z,z) + I_q(z,z) = 1.$$

Και τότε:

$$P(z) = 2I_q(z,z)$$

Σε τελικό στάδιο χρησιμοποιούμε:

$$I_q(z,z) = \frac{1}{2} I_s(z, \frac{1}{2}), \text{ όπου } s = 4pq < 1 \text{ και τελικά}$$

$$P(z) = 2 \cdot I_q(z,z) = 2 \cdot \frac{1}{2} \cdot I_s\left(z, \frac{1}{2}\right) = I_s(z, \frac{1}{2}) \blacksquare$$

<u>Σημείωση:</u>

Στο χώρο των πραγματικών αριθμών, η πιθανότητα αυτή ισούται με τη πιθανότητα επιτυχίας της επίθεσης■

Από την ασυμπτωτική ανάλυση θα χρησιμοποιηθούν δύο πολύ χρήσιμα λήμματα. Συγκεκριμένα, γνωρίζω:

Λήμμα 1: Για συνάρτηση $f \in C^1(R+)$ $με$ $f(0) \neq 0$ απολύτως συγκλίνουσα και ολοκληρώσιμη, ισχύει καθώς το $z \to \infty$:

$$\int_0^{+\infty} f(u)e^{-zu}du \sim \frac{f(0)}{z}.$$

Λήμμα 2: Για $b > 0$ και $s \in [0,1]$, όταν $z \gg 1$, ισχύει:

$$B_s(z,b) \sim \frac{s^z}{z}(1-s)^{b-1}.$$

(Απόδειξη): Αρχικά θέτω την μεταβλητή $u = \ln(\frac{s}{t})$, την οποία σε επόμενη φάση θα αντικαταστήσω στην κατανομή $B_s(z,b) = \int_0^s t^{z-1}(1-t)^{b-1}dt$.

Λόγω $u = \ln(\frac{s}{t})$, έχω:

$$e^u = \frac{s}{t} \Leftrightarrow t = se^{-u} \text{ και παραγωγίζοντας προκύπτει } dt = -se^{-u}du.$$

Τώρα αντικαθιστώντας τις t, dt ποσότητες στην $B_s(z,b)$, προκύπτει:

$$B_s(z,b) = \int_0^s t^{z-1}(1-t)^{b-1}dt \Leftrightarrow$$

$$\int_0^s (se^{-u})^{z-1}(1-se^{-u})^{b-1}(-se^{-u})du \Leftrightarrow$$

$$\int_0^s s^{z-1}e^{-u(z-1)}(-se^{-u})(1-se^{-u})^{b-1}du \Leftrightarrow$$

$$\int_0^s \frac{s^z}{s}e^{-uz+u}(-se^{-u})(1-se^{-u})^{b-1}du \Leftrightarrow$$

$$s^z\int_0^s \frac{1}{s}e^u(-se^{-u})e^{-uz}(1-se^{-u})^{b-1}du \Leftrightarrow$$

$$s^z\int_0^s \frac{-se^{-u}e^u}{s}e^{-uz}(1-se^{-u})^{b-1}du \Leftrightarrow$$

$$-s^z\int_0^s e^{-zu}(1-se^{-u})^{b-1}du \Leftrightarrow$$

Και λόγω ότι μιλάμε για ποσότητα που αντιπροσωπεύει πιθανότητα το θεωρούμε θετικό, οπότε:

$$s^z \int_0^{+\infty} e^{-zu}(1-se^{-u})^{b-1}du, \text{ όταν το } s \to \infty.$$

Τέλος χρησιμοποιώντας το λήμμα1 για $f(u) = (1-se^{-u})^{b-1}$, έχω

$$B_s(z,b) \sim \frac{f(0)}{z} s^z = \frac{(1-s)^{b-1}s^z}{z} \blacksquare$$

Συνέπεια του παραπάνω θεωρήματος είναι η περίπτωση όπου s= $4pq < 1$, καθώς το z → ∞, έχουμε:

$$P(z) \sim \frac{s^z}{\sqrt{\pi(1-z)s}}$$

(Απόδειξη): Από την αναφερθείσα φόρμουλα του Stirling, γνωρίζουμε ότι:

$$B\left(z,\frac{1}{2}\right) = \frac{\Gamma(z)\Gamma(\frac{1}{2})}{\Gamma(z+\frac{1}{2})} \sim \sqrt{\frac{\pi}{2}}$$

Οπότε λόγω:

$$P(z) = I_s\left(z,\frac{1}{2}\right) = \frac{B_s\left(z,\frac{1}{2}\right)}{B(z,\frac{1}{2})}$$

$$P(z) \sim \frac{(1-s)^{-\frac{1}{2}}\frac{s^z}{z}}{\sqrt{\frac{\pi}{2}}} \sim \frac{s^z}{\sqrt{\pi(1-s)z}}$$

Για την παραπάνω μελέτη θεωρούμε τον παράγοντα χρόνο αμελητέα ποσότητα, πράγμα που κρατά τα αποτελέσματα αυτά σε καθαρό θεωρητικό επίπεδο.

<u>Θεώρημα</u>: Συμβολίζοντας με $P(z,t)$ την πιθανότητα επιτυχίας μιας επίθεσης διπλής δαπάνης, όταν z blocks έχουν μέχρι εκείνη την στιγμή t επικυρωθεί. Βάσει των προηγουμένων η πιθανότητα υπολογίζεται ως:

Καθώς το $z \to \infty$, πάλι για $s = 4pq < 1$, λόγω της προηγούμενη συνέπειας θέτοντας $\lambda = \frac{q}{p}$ και $c(\lambda) = \lambda - 1 - log(\lambda) > 0$,τότε:

$$P_{SN}(z) \sim e^{-\frac{z\left(\frac{q}{p}-1-ln\left(\frac{q}{p}\right)\right)}{2}} = \frac{e^{-zc(\lambda)}}{2},$$

Και παρατηρούμε ότι $-log(s) > c(\lambda)$ που σημαίνει ότι $P_{SN}(z) < P(z)$ για z αρκετά μεγάλο.

2.2 Η ανάλυση των δημιουργών του Bitcoin

Εναλλακτικά θεωρώντας t, τον απαιτούμενο χρόνο δημιουργίας z block(s), για $z \in N$, όπου N το σύνολο των φυσικών αριθμών, γνωρίζουμε ότι αν μέχρι το z^{th} block ο επιτιθέμενος έχει δημιουργήσει k blocks τότε δύο είναι τα πιθανά σενάρια:

- Για $k > z$ ο επιτιθέμενος καταφέρνει να πείσει την κοινότητα και να αντικατασταθεί το blockchain με την δικιά του ψευδή αλυσίδα.
- Για $k \leq z$, η επίθεση αποτυγχάνει ενώ στην οριακή φάση που συντρέχουν η πιθανότητα επιτυχίας της επίθεσης είναι $\left(\frac{q}{p}\right)^z$ όπως υπολογίστηκε προηγουμένως στα μαθηματικά εξόρυξης.

Οπότε η πιθανότητα P της επιτυχίας του επιτιθέμενου είναι:

$$P = P[N'(S_z) \geq z] + \sum_{k=0}^{z-1} P[N'(S_Z) = k] \cdot q_{z-k}$$

Ορισμός1: Για $n \in Z$. Δηλώνουμε με την μεταβλητή q_n την πιθανότητα ο επιτιθέμενος κακόβουλος χρήστης να προλάβει τους ανθρακωρύχους και να ενημερώσει την δικιά του αλυσίδα, από την στιγμή που εκείνη είναι n block πίσω.

$$q_n = \left(\frac{q}{p}\right)^n,$$

Και όπως πριν συμβολίζουμε, για $z \in Z$, την πιθανότητα να επιτύχει η επίθεση, ως P(z).

Σημείωση: Για αρχική τιμή $t = 0$, μια επίθεση διπλής δαπάνης δεν μπορεί να επιτύχει πριν από την χρονική στιγμή $t = S_z$.

Το σημείο στο οποίο οι δημιουργεί έκαναν λάθος είναι ότι θεώρησαν πως η εξόρυξη των block γίνεται στον αναμενόμενο χρόνο, κάτι το οποίο ισχύει μόνο όταν $z \to \infty$. Δηλαδή:

$$t_z = E[S_z] = zE[T] = z\frac{\tau_0}{p}$$

Από την ανάλυση στην εξόρυξη, είχαμε:

$$\lambda = a't_z = \frac{za'\tau_0}{p} = z\frac{q}{p}$$

Ουσιαστικά, βάσει των παραπάνω ο παραλήπτης περιμένει μέχρι η συναλλαγή του να προστεθεί μεταξύ των υπολοίπων σε ένα block και έπειτα να επικολληθούν z block από πίσω του. Παρόλο που δεν γνωρίζει τη μέχρι τότε πρόοδο του επιτιθέμενου hacker, εμπιστευόμενος το χρόνο

επικύρωσης των block των ανθρακωρύχων, οφείλει να γνωρίζει ότι ο επιτιθέμενος θα έχει κάνει πρόοδο η οποία ακολουθεί την κατανομή Poisson με παράμετρο λ.

Και θεωρώντας $N'(S_Z) = N'(t_z)$ υπολογίζω ως εξής:

$$P_{SN}(z) = P[N'(t_z) \geq z] + \sum_{k=0}^{z-1} P[N'(t_z) = k] \cdot q_{z-k} \Leftrightarrow$$

$$P_{SN}(z) = 1 - \sum_{k=0}^{z-1} P[N'(t_z) = k] + \sum_{k=0}^{z-1} P[N'(t_z) = k] \cdot q_{z-k} \Leftrightarrow$$

$$P_{SN}(z) = 1 \sum_{k-0}^{z-1} e^{-\lambda} \frac{\lambda^k}{k!} (1 - q_{z-k}).$$

<u>Υπενθύμιση</u>: Ισχύει από την προηγούμενη ανάλυση που έγινε στην διαδικασία εξόρυξης για την ποσότητα $P[N'(t_z) = k]$:

$$P[N(t) = k] = \frac{(at)^k}{k!} e^{-at}, \text{ άρα θα έχω για } \lambda = a't_z:$$

$$P[N'(t_z) = k] = e^{-\lambda} \frac{\lambda^k}{k!}.$$

<u>Σημείωση:</u> Σε κάθε περίπτωση $P(z) \neq P_{SN}(z)$, από την στιγμή που $N'(S_z) \neq N'(E[S_Z])$!

Σε γενικές γραμμές η παραπάνω ανάλυση έχει χαρακτηριστεί εσφαλμένη κυρίως λόγο του ελλιπούς θεωρητικού υποβάθρου, από μεριάς των δημιουργών του Bitcoin, όμως αναμφίβολα απετέλεσε δομικό υλικό των παρακάτω αναλύσεων.

2.2.1 Απόδειξη εργασίας (Proof of work)

Η απόδειξη εργασίας, γνωστότερή από την ξένη βιβλιογραφία ως proof of work, είναι ένα οικονομικό μέτρο με στόχο την αποτροπή άρνησης παροχής υπηρεσιών και γενικότερα παραβιάσεων όπως το spamming, το οποίο εφαρμόζεται σε ένα δίκτυο χρηστών. Απαιτείται η παροχή υπηρεσιών από τους αιτούντες χρήστες, η οποία μεταφράζεται συνήθως σε διαδικασίες επεξεργασίας, μέσω υπολογιστικών συστημάτων. Οι διαδικασίες είναι ουσιαστικά επιλύσεις γρίφων, δύσκολοι στην επίλυση όχι όμως ανέφικτοι και επιπλέον εύκολοι στην επαλήθευση.

Στη περίπτωση του Bitcoin, οι ομάδες ανθρακωρύχων(miners) χρησιμοποιούν τα πολύ ισχυρά και εξιδεικευμένα υπολογιστικά τους συστήματα για να επιλύσουν τους γρίφους κατακερματισμού(hash puzzles), η χρήση των οποίων είναι η ιδέα της απόδειξης εργασίας. Για να δημιουργηθεί νέο block, ο ανθρακωρύχος που προτείνει αυτό το block είναι υποχρεωμένος να

βρει έναν αριθμό που να ικανοποιεί την διαδικασία κατακερματισμού – hash. Η ίδια η πλατφόρμα συγκεκριμενοποιεί το πρόβλημα που πρέπει να λυθεί, καθώς επίσης και την αμοιβή των ανθρακωρύχων ανά χρονικά διαστήματα. Συγκεκριμένα:

$$F(x \mid y) < Target < -(target), όπου$$

- $X = x_1|x_2|x_3|x_4|x_5$ $με$ $\begin{cases} x_1 = Version \\ x_2 = Hash\ του\ Block \\ Hash\ της\ ρίζας\ του\ δέντρου\ Merkle \\ Target\ of\ the\ Timestamp \end{cases}$
- $Κεφαλή\ του\ Block = x|y$

Όσον αφορά το κόστος εξόρυξης, επιθυμούμε να είναι παραμετροποιήσιμο, διότι όλο και περισσότεροι ανθρακωρύχοι συμμετέχουν στην εξόρυξη ή αναπτύσσουν ταχύτερα και γρηγορότερα τις δομές τους, πράγμα που σημαίνει ότι σε δεδομένο χρονικό διάστημα θα επαληθευτούν περισσότερα hasharίσματα από τα αναμενόμενα. Αυτό θα οδηγούσε την πλατφόρμα σε προβλήματα για τα οποία θα απαιτούνταν αναπροσαρμογές ακόμα και στο πηγαίο κώδικα. Έτσι, το Bitcoin αναπροσαρμόζει αυτόματα τον στόχο οπότε η δυσκολία άρα και η ποσότητα κατακερματισμού αυξάνεται με αποτέλεσμα να διατηρείται μια ισορροπία.

Βάση όλων των παραπάνω, ένα bitcoin ουσιαστικά είναι μια αλυσίδα από ψηφιακές υπογραφές, όπου κάθε ιδιοκτήτης μεταφέρει το νόμισμα στον επόμενο, υπογράφοντας ψηφιακά το αποτέλεσμα κατακερματισμού της προηγούμενης συναλλαγής hash καθώς και το δημόσιο κλειδί του νέο κατόχου. Στη συνέχεια γίνεται η προσθήκη των νομισμάτων στο νέο λογαριασμό. Μερικοί από τους δικαιούχους μπορούν να επαληθεύσουν τις υπογραφές και κατά συνέπεια την αλυσίδα (blockchain).

$$\mathbf{Transaction = 2\ Scripts = Scriptsign + scriptpk}$$

Γενικά για την επίσημη αλυσίδα των κόμβων(blockchain) θα ισχύει:

Για (B_i), όπου $0 \leq i \leq N$, ώστε $\sum_{i=0}^{N} D_i$να μεγιστοποιείται για D_i τη δυσκολία του κόμβου B_i.

2.3 Η ανάλυση του Meni Rosenfeld

Οι παραδοχές των δημιουργών του νομίσματος αποδείχθηκαν το 2012 εσφαλμένες μέσα από την μελέτη του Meni Rosenfeld, αναλυτή και επιχειρηματία που δραστηριοποιείται στο χώρο των ψηφιακών νομισμάτων. Συγκεκριμένα στηριζόμενος στις μέχρι τότε εικασίες τους υπολόγισε τις πιθανότητες που αφορούν την επίθεση διπλής δαπάνης ρίχνοντας έτσι περισσότερο “φώς” στο κίνδυνο που εγκυμονεί, παρά την πεποίθηση ότι μια τέτοια προσπάθεια θα εγκλωβιζόταν αποτελεσματικά από την ομοφωνία της κοινότητας και την απόδειξη εργασίας των ανθρακωρύχων (proof of work).

(Θεωρητικό υπόβαθρο): Θέτουμε $X_n = N'(S_n)$ τον αριθμό των block που φτιάχνουν οι επιτιθέμενοι την χρονική στιγμή που οι ανθρακωρύχοι έχουν μόλις εξορύξει το n^{th} block.

Πρόταση: Η $X_n \coloneqq N'(S_n)$, η τυχαία μεταβλητή X_n ακολουθεί αρνητική διωνυμική κατανομή με παραμέτρους (n, p), για $k \geq 0$. Δηλαδή:

$$P[X_n = k] = p^n q^k \binom{k+n-1}{k}$$

(Απόδειξη): Γνωρίζουμε ότι $S_n \sim \Gamma(a, n)$, δηλαδή:

$$f_{S_n}(t) = \frac{a^n}{(n-1)!} t^{n-1} e^{-at},$$

όπου $f_{S_n}(t)$ είναι η συνάρτηση πυκνότητας πιθανότητας της ποσότητας S_n. Οπότε:

$$P[X_n = k] = \int_0^\infty P\big[N'(S_n) = k \big| S_n \in [t, t+dt]\big] \cdot P\big[S_n \in [t.\, t+dt]\big] \Leftrightarrow$$

$$P[X_n = k] = \int_0^\infty P[N'(S_n) = k | S_n = t]\, f_{S_n}(t) dt \Leftrightarrow$$

$$P[X_n = k] = \int_0^\infty P[N'(t) = k] \cdot f_{Sn}(t) dt$$

$$= \int_0^\infty \frac{(a't)^k}{k!} e^{-a't} \frac{a^n}{(n-1)!} t^{n-1} e^{-at} dt$$

$$= \frac{1}{(n-1)!\, k!} \int_0^\infty t^{k+n-1} \frac{(a')^k}{e^{a't}} \frac{a^n}{e^{at}} dt$$

$$= \frac{p^n q^k}{(n-1)!\, k!} \int_0^\infty t^{k+n-1} dt$$

$$= \frac{p^n q^k}{(n-1)!\, k!} (k+n-1)!$$

$$= p^n q^k \binom{k+n-1}{k} \blacksquare$$

που είναι η ζητούμενη ποσότητα. Όσον αφορά τις πράξεις που παραλείφθηκαν υπενθυμίζεται ότι:

- $P[N(t) = k] = \frac{(at)^k}{k!} e^{-at}$, οπότε η δεσμευμένη πιθανότητα του ενδεχομένου είναι:

$$P[N'(S_n) = k | S_n = t] = \frac{(a't)^k}{k!} e^{-a't}.$$

- Από τον ολοκληρωτικό λογισμό $\int_0^\infty t^{k+n-1} dt = (k+n-1)!$
- Ισχύει για τους παραγοντικούς αριθμούς:
  - $\binom{k+n-1}{k} = \frac{(k+n-1)!}{(n-1)!k!}$

- Οι πιθανότητες p, q, ακολουθούν εκθετική κατανομή με παραμέτρους a, a' αντίστοιχα.

Συμπέρασμα: Η τυχαία μεταβλητή X_n δεν ακολουθεί τον Νόμο του Poisson με παράμετρο $\frac{nq}{p}$, όπως θεώρησαν οι δημιουργοί. Παρακάτω δίνεται το θεώρημα σύμφωνα με το οποίο μόνο ασυμπτωτικά έχουμε μια σύγκλιση με την κατανομή Poisson. Συγκεκριμένα:

Θεώρημα: Καθώς το $n \to \infty$, για $q \to 0$ όταν $l_n = \frac{nq}{p} \to \lambda$, ισχύει:

$$P[X_n = k] \to \frac{\lambda^k}{k!} e^{-\lambda}$$

(Απόδειξη): Έχουμε από πριν:

$l_n = \frac{nq}{p}$, σχέση η οποία μας οδηγεί στο ζεύγος των σχέσεων $\begin{cases} p = \frac{n}{n+l_n} \\ q = 1 - p = \frac{l_n}{n+l_n} \end{cases}$

Διότι:

1. $l_n = \frac{nq}{p}$, οπότε $pl_n = nq \Leftrightarrow pl_n = n(1-p) \Leftrightarrow p = \frac{n-np}{l_n} \Leftrightarrow pl_n + np = n \Leftrightarrow p = \frac{n}{n+l_n}$.
2. $q = 1 - p = 1 - \frac{n}{(n+l_n)} = \frac{l_n}{n+l_n}$.

Προχωρώντας λοιπόν στο ζητούμενο, έχουμε:

$$P[X_n = k] = \frac{n^n}{(n+l_n)^n} \frac{l_n^k}{(n+l_n)^k} \frac{(k+n-1)!}{(n-1)!\,k!} \Leftrightarrow$$

$$\frac{l_n^k}{k!} \frac{1}{\left(1+\frac{l_n}{n}\right)^n} \frac{n(n+1)(n+2)\dots(n+k-1)}{(n+l_n)^k} \Leftrightarrow$$

$$\text{όπου για } n \to \infty, \text{καταλλήγουμε στο ζητούμενο } P[X_n = k] \cong \frac{\lambda^k}{k!} e^{-\lambda} \blacksquare$$

Υπενθυμίζεται ότι:

- $\lim_{n\to\infty} \left(1 + \frac{l_n}{n}\right)^n = e^{\lambda}$
- Από την εκφώνηση $\lim_{\nu\to\infty} l_n = \lambda$, άρα $\lim_{n\to\infty} \frac{l_n^k}{k!} = \frac{\lambda^k}{k!}$
- $\lim_{n\to\infty} \frac{n(n+1)(n+2)\dots(n+k-1)}{(n+l_n)^k} = \frac{\infty}{\infty} = 1$

Οπότε μπορούμε να υπολογίσουμε την πιθανότητα επιτυχίας ενός hacker, χρησιμοποιώντας την παραπάνω πρόταση πάνω στο γεγονός ότι:

$$P(z) = 1 - \sum_{k=0}^{z-1} P[N'(S_Z) = k](1 - q_{z-k}).$$

Προκύπτει:

(Βήμα 1):

$$P[N'(S_z = k)](1 - q_{z-k}) = P[X_z = k](1 - q_{z-k})$$

Άρα έχω:

$$P(z) = \sum_{k>z} p^z q^k \binom{k+z-1}{k} + \sum_{k=0}^{z} \binom{q}{p}^{z-k} p^z q^k \binom{k+z-1}{k}$$

$$P(z) = 1 - \sum_{k=0}^{z-1} p^z q^k \binom{k+z-1}{k}(1 - q_{z-k}) \Leftrightarrow$$

(Βήμα 2):

Γνωρίζω από την σχέση επαναληπτικότητας $q_n = qq_{n-1} + pq_{n+1}$, ότι:

$$q_n = \min\left(\frac{q}{p}, 1\right)^{\max(n+1,0)} = \begin{cases} 1, & \text{όταν } n < 0 \text{ ή } q > p \\ \left(\frac{q}{p}\right)^{n+1}, & \text{όταν } n \geq 0 \text{ και } q \leq p \end{cases}$$

Άρα έχω:

$$p^z q^k (1 - q_{z-k}) =$$

$$p^z q^k - p^z q^k q_{z-k} =$$

$$p^z q^k - p^z q^k \frac{q^{z-k+1}}{p^{z-k+1}}$$

$$\cong p^z q^k - p^k q^z$$

Τελικά:

$$P(z) = 1 - \sum_{k=0}^{z-1} (p^z q^k - q^z p^k) \binom{k+z-1}{k} \blacksquare$$

Που δεν είναι άλλη από την πιθανότητα επιτυχίας μια επίθεσης διπλής δαπάνης. Με διαφορετικές τιμές του q, μελετάται η διαφορά στις τιμές των $P(z)$ & $P_{SN}(z)$.

2.4 Κόστος επίθεσης διπλής δαπάνης

Σε γενικές γραμμές, σε χρονικό διάστημα t για ικανότητα κατακερματισμού h με συνολικό κόστος C, η σχέση που συνδέει τα παραπάνω μεγέθη είναι:

$$\exists \lambda > 0, \dot{\omega}\sigma\tau\varepsilon\ C(h,t) = \lambda h t$$

Συμπεραίνουμε λοιπόν ότι η σχέση κόστους και hashing power είναι γραμμική για ένα δεδομένο χρονικό διάστημα. Φυσικά δεν θα έπρεπε να παραλείψουμε και την αμοιβή ανά block $B = 12.5\ bitcoins$. Η τιμή λ, επαναπροσδιορίζεται προκυμμένου να ισχύει:

$$C(h+h', \tau_0) = B \Leftrightarrow \lambda(h+h')\tau_0 = B, \text{ οπότε}$$

$$\lambda = \frac{B}{(h+h')\tau_0}$$

Και υπενθυμίζοντας ότι $p = \frac{a}{a+a'} \rightarrow p = \frac{h}{h+h'}$ τότε $C(h,t) = \frac{ht}{(h+h')\tau_0} B = \frac{pt}{\tau_0} B$.

Στη περίπτωση που μελετάμε το κόστος σε τελικό χρόνο $\tau := Inf\{t \geq \frac{S_Z}{N'(t)} \geq N(t)\}$, τότε:

$$C = E\left[\frac{q\tau}{\tau_0} B\right] = \frac{qB}{\tau_0} E[\tau] = +\infty.$$

Στην ειδική περίπτωση όπου $\tau_T := Inf\{t \geq \frac{S_Z}{N'(t)} \geq N(t)\} \cap T$, θεωρούμε ότι η επίθεση τελειώνει όταν είτε ο επιτιθέμενος φτάσει στα $z+1$ block στην απατηλή αλυσίδα, είτε όταν οι ανθρακωρύχοι δημιουργήσουν $z+1$ block πάνω στην βασική αλυσίδα του blockchain. Η διαμάχη προβλέπεται να λάβει τέλος σε χρόνο:

$$\tilde{\tau} := S_{z+1} \cap S'_{z+1},$$

και το κόστος τότε υπολογίζεται σε:

$$C = E\left[\frac{q\tilde{\tau}}{\tau_0} B\right] = \frac{qB}{\tau_0} E[S_{z+1} \cap S'_{z+1}].$$

Υπενθύμιση: Οι ποσότητες S_{z+1} *και* S'_{z+1}, είναι ανεξάρτητες τυχαίες μεταβλητές που ακολουθούν κατανομή Γάμμα.

Επίλογος: Οι συναλλαγές που πραγματοποιούνται στη πλατφόρμα και αποθηκεύονται στην διαχρονική και πλήρως επεξηγηματική αλυσίδα του blockchain προστατεύονται αποτελεσματικότερα με την αύξηση του αριθμού των επικυρώσεων που τίθενται από το σύστημα αλλά και τους χρήστες. Ο επιτιθέμενος δυσκολεύεται σε μεγάλο βαθμό από την απόδειξη εργασίας που πραγματοποιείται από την κοινότητα των ανθρακωρύχων, χωρίς αυτό να σημαίνει ότι δεν υπάρχει δυνατότητα πλαστογράφησης της αλυσίδας ή παράκαμψης των

διαδικασιών. **Η συνεχείς επίβλεψη και αναδιαμόρφωση του πηγαίου κώδικα αποτελεί την μόνη λύση στο πρόβλημα του hacking, το οποίο μέχρι και το τέλος του νομίσματος θα είναι επικίνδυνο για όλη την κοινότητα.**

2.5 Ανάλυση κινδύνου

Θέλοντας να εξετάσουμε βαθύτερα το πρόβλημα εισάγουμε μια καινούργια παράμετρο στο πρόβλημα της επίθεσης διπλής δαπάνης. Συγκεκριμένα θεωρούμε πλέον ότι η πιθανότητα να επιτύχει μια επίθεση διπλής δαπάνης, αυξάνεται ανάλογα με το χρονικό διάστημα τ_1, που χρειάζεται να επικυρωθούν μέχρι τότε z συναλλαγές.

Θεωρούμε ότι οι επιτιθέμενοι έχουν περισσότερο χρόνο στη διάθεση τους για να εξορύξουν την απατηλή αλυσίδα την οποία θα προσπαθήσουν να εισάγουν στο blockchain. Βέβαια αν οι επικυρώσεις(έπειτα από τις εξορύξεις των ανθρακωρύχων) συμβούν γρηγορότερα από τον αναμενόμενο χρόνο, τότε η επίθεση δύσκολα θα επιτύχει.

- Η τιμή τ_1 είναι ως ένα βαθμό γνωστή (προβλέπεται από μαθηματικές λύσεις). Η υπό προϋποθέσεις πιθανότητα για φαινομενικά γνωστό τ_1, είναι:
  i. $\kappa = \frac{\tau_1}{zt_0} = \frac{p\tau_1}{z\tau_0} > 0.$
  ii. Όπου κ είναι μια παράμετρος που υπολογίζει την απόκλιση από τον μέσο χρόνο t_0, που χρειάζεται για να επικυρωθούν τα block από τους ανθρακωρύχους.

Υπενθύμιση: Ο χρόνος $t_0 = \frac{\tau_0}{p}$, όπου $\tau_0 = 600\ sec.$

Σε γενικές γραμμές ο μέσος χρήστης-λήπτης μιας συναλλαγής για να προστατευθεί από τέτοιου είδους επιθέσεις θα πρέπει να περιμένει να γίνουν τουλάχιστον z επιβεβαιώσεις. Σκοπός της όλης έρευνας είναι να υπολογιστεί η πιθανότητα $P(z, \kappa)$ επιτυχίας των επιτιθέμενων.

Υπενθύμιση: Από τους δημιουργούς του Bitcoin είχαμε:

$$P_{SN}(z) = P(z, 1)$$

Θεώρημα: Ισχύουν οι εξής πιθανότητες,

- $P(z, k) = 1 - Q\left(z, \frac{kzq}{p}\right) + \left(\frac{q}{p}\right)^z e^{kz\frac{p-q}{p}} Q(z, kz).$
- $P_{SN}(z) = P(z, 1) = 1 - Q\left(z, \frac{zq}{p}\right) + \left(\frac{q}{p}\right)^z e^{z\frac{p-q}{p}} Q(z, z).$

(Απόδειξη): Από τις προηγούμενες αναλύσεις των δημιουργών και της διαδικασίας εξόρυξης, έχουμε:

- $\lambda(z,k) = a'\tau_1$, *όπου* $\alpha' = \frac{q}{\tau_0}$ *και* $p = \frac{\tau_0}{t_0}$, *άρα* $\lambda(z,k) = \frac{q}{\tau_0} \cdot \kappa z t_0$. Συνεχίζοντας τις πράξεις:

$$\lambda(z,\kappa) = \frac{\kappa z q\ t_0}{\tau_0} = \kappa z q/p$$

- $P[N'(\tau_1) = k] = \frac{(\alpha'\tau_1)^k}{k!} e^{(-\alpha'\tau_1)}$, *όπου για* $\kappa = 1$, υπολογίζεται η πιθανότητα των δημιουργών.

Οπότε από τις παραπάνω σχέσεις προκύπτει:

$$P[N'(\tau_1) = k] = \frac{\left(\frac{zq}{p}\kappa\right)^k}{k!} e^{\left(-\frac{zq}{p}\right)\kappa}.$$

Από τις κατανομές των τυχαίων μεταβλητών υπενθυμίζεται η μη-ολοκληρώσιμη κανονικοποιημένη μορφή της συνάρτησης Γάμμα:

- $Q(s,x) = \frac{\Gamma(s,x)}{\Gamma(x)}$, με $\Gamma(s,x) = \int_x^\infty t^{s-1}e^{-t}dt$ οπότε: $Q(z,\lambda) = \sum_{k=0}^\infty \frac{\lambda^k}{k!} e^{-\lambda}$.

Οπότε:

$$P(z,\kappa) = \sum_{k=z}^{\infty} \frac{\left(\lambda(z,\kappa)\right)^k}{k!} e^{-\lambda(z,\kappa)} + \sum_{k=0}^{z-1} \left(\frac{q}{p}\right)^{z-k} \frac{\left(\lambda(z,\kappa)\right)^k}{k!} e^{-\lambda(z,\kappa)} \Leftrightarrow$$

$$P(z,\kappa) = 1 - \sum_{k=0}^{z-1} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right) \frac{\left(\lambda(z,\kappa)\right)^k}{k!} e^{-\lambda(z,\kappa)} \Leftrightarrow$$

$$P(z,\kappa) = 1 - Q\left(z, \frac{\kappa z p}{p}\right) + \left(\frac{q}{p}\right)^z e^{\frac{\kappa z(p-q)}{p}} Q(z,\kappa z) \blacksquare$$

***(Θεωρητικό υπόβαθρο)*:** Θέλοντας να δώσουμε έμφαση στις $P(z)$ και $Q(z,x)$ παρακάτω αναφέρεται η διαδικασία εύρεσης των τύπων.

<u>Θεώρημα</u>: Ισχύει για:

$$P(z) = \int_0^\infty P(z,\kappa) dp(\kappa)\,, \text{όπου } dp_z(\kappa) = \frac{z^z}{(z-1)!}\ k^{z-1}e^{-z\kappa}d\kappa.$$

Αποδεικνύεται μέσω του Mathematica ότι:

$$\int_0^\infty \frac{z^z}{(z-1)!} \kappa^{z-1}e^{-\kappa z}d\kappa = 1.$$

<u>Παρατήρηση</u>: Η απόδειξη παραλείπεται, διότι δεν εξυπηρετεί τους σκοπούς της έρευνας.

Τότε μπορεί κανείς να γράψει:

$$P(z) = 1 - \sum_{k=0}^{z-1} f_k(\kappa)\,, \mu\varepsilon\ f_k(\kappa) = \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)\frac{\left(\frac{zq}{p}\right)^k}{k!}\kappa^k e^{\frac{zq\kappa}{p}}.$$

Οπότε εύκολα όπως και πριν καταλήγουμε στη σχέση:

***Λήμμα*:** Για$k \geq 0$, έχουμε:

$$\int_0^\infty f_k(\kappa)dp_z(\kappa) = (p^z q^k - q^z p^k)\binom{k+z-1}{k}$$

(Απόδειξη): Θέτω την τυχαία μεταβλητή $\kappa = \frac{p}{z\tau_0}S_Z$. Όπως προαναφέραμε για τις ποσότητες κ, S_z γνωρίζουμε ότι $S_Z \sim \Gamma(z,a)\ και\ \Gamma\left(z, \alpha\frac{z\tau_0}{p}\right) = \Gamma(z,z)$. Προφανώς η πυκνότητα dp_z είναι η κατανομή της ποσότητας κ. Αρκεί να αποδείξουμε ότι:

$$P(z) = E[P(z,\kappa)].$$

Έχω από προηγούμενες αναλύσεις:

$$P(z) = P[N'(S_z) \geq z] + \sum_{k=0}^{z-1} P[N'(S_z) = k]\cdot q_{z-k} \ \Leftrightarrow$$

$$P(z) = 1 - \sum_{k=0}^{z-1}(1 - q_{z-k})P[N'(S_z) = k] \ \Leftrightarrow$$

Λόγω προηγουμένων αποδείξεων γνωρίζω:

- $E[\kappa] = 1$
- $q_{z-k} = \left(\frac{q}{p}\right)^{z-k}$
- $Q(z,x) = \sum_{k=0}^{z-1}\frac{x^k}{k!}e^{-x}$.
- $P[N'(S_z) = k|S_z] = \frac{(a'S_z)^k}{k!}e^{a'S_z}$

Προκύπτει:

$$P(z) = 1 - E[\sum_{k=0}^{z-1}\frac{(a'S_z)^k}{k!}e^{-a'S_z}] + \left(\frac{q}{p}\right)^z E[e^{a'\frac{p-q}{q}S_z}\sum_{k=0}^{z-1}\frac{\left(\frac{a'p}{q}S_z\right)^k e^{-\frac{a'p}{q}S_z}}{k!}] \ \Leftrightarrow$$

$$P(z) = E\left[1 - Q\left(z, \frac{zq}{p}\kappa\right) + \left(\frac{q}{p}\right)^z e^{z\left(1-\frac{q}{p}\right)\kappa} Q(z, z\kappa)\right] \Leftrightarrow$$

$$P(z) = E[P(z, \kappa)]$$

■

2.6 Ασυμπτωτική μελέτη των $\mathbf{P(z, \kappa)}$ & $\mathbf{P_{SN}(z)}$

Μελετώντας την ποσότητα $Q(z, \lambda z)$, καθώς το $z \to +\infty$ για διαφορετικές τιμές του $\lambda > 0$. Προκύπτουν διάφορα αξιοσημείωτα αποτελέσματα. Παρακάτω παρατίθενται λήμματα και προτάσεις που τις αναλύουν.

(Θεωρητικό Υπόβαθρο): Μέσα από την χρήση της θεωρίας του Stirling έχουν προκύψει οι εξής βοηθητικοί τύποι για την μη ολοκληρώσιμη κανονικοποιημένη Γάμμα κατανομή:

- $\Gamma(z) = \sqrt{\frac{2\pi}{z}}\left(\frac{z}{e}\sqrt{zsin\left(\frac{1}{z}\right) + \frac{1}{810z^6}}\right)^z = \sqrt{\frac{2\pi}{z}}\left(\frac{z}{e}\right)^z\left(1 + o\left(\frac{1}{z}\right)\right)$
- $Q(z, z) = \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}}{(z-1)!} \cong \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}}{(z-1)!}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o\left(z^{-\frac{1}{2}}\right)\right)$
- $Q(z, \lambda z) = \frac{\Gamma(z,\lambda z)}{\Gamma(z)} \sim \frac{(\lambda z)^z e^{-(z\lambda)}}{z!(\lambda-1)}$

<u>Λήμμα</u>: Έχουμε:

a) Για $0 < \lambda < 1$, όταν $Q(z, \lambda z) \to 1$ $\kappa\alpha\iota$ $1 - Q(z, \lambda z) \sim \frac{1}{1-\lambda}\frac{1}{\sqrt{2\pi z}}e^{-z(\lambda-1-log\lambda)}$

(Απόδειξη): Από την φόρμουλα του Stirling με τις παραπάνω υποθέσεις έχω:

Αρχικά έχω:

$$\lim_{z\to\infty} Q(z, z) = \lim_{z\to\infty}\left(\frac{(\lambda z)^z e^{-(z\lambda)}}{z!(\lambda-1)}\right) = 1, \text{ από το Mathematica.}$$

$$1 - Q(z, \lambda z) = 1 - \frac{\Gamma(z, \lambda z)}{\Gamma(z)} \sim \frac{z^z \lambda^z e^{-z\lambda}}{z!\,(1-\lambda)} \sim \frac{1}{1-\lambda}\frac{1}{\sqrt{2\pi z}}e^{-z(\lambda-1-log\lambda)}$$ ■

b) Για $\lambda = 1, Q(z, z) \to \frac{1}{2}$ $\kappa\alpha\iota$ $\frac{1}{2} - Q(z, z) \sim \frac{1}{3\sqrt{2\pi z}}$

(Απόδειξη): Πάλι από την φόρμουλα του Stirling, προκύπτει ως εξής:

Αρχικά έχω:

$$\lim_{z\to\infty} Q(z,z) = lim_{z\to\infty}\left(\frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}}{(z-1)!}\right) = \frac{1}{2},$$ αποτέλεσμα από το Mathematica

<u>Υπόδειξη</u>: Η σειρά $\sum_{z=1}^{\infty} Q(z,z) = \frac{1}{2} - \frac{1}{24z} + \frac{1}{576z^2} + \frac{139}{103680z^3} - \frac{571}{4976640z^4} + o\left(\left(\frac{1}{2}\right)^5\right)$.

Έπειτα προκύπτει:

$$Q(z,z) = \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}}{(z-1)!} \Leftrightarrow$$

$$Q(z,z) = \frac{z^{z}e^{-z}\sqrt{\frac{\pi z}{2}}}{z(z-1)!} = \frac{\sqrt{2}\left(\frac{z}{e}\right)^{z}\sqrt{\pi z}}{2z!} = \frac{1}{2}\frac{\left(\frac{z}{e}\right)^{z}\sqrt{2\pi z}}{z!} \Leftrightarrow$$

$$\lim_{z\to\infty} Q(z,z) = \frac{1}{2}\cdot\lim_{z\to\infty}\left(\frac{\left(\frac{z}{e}\right)^{z}\sqrt{2\pi z}}{z!}\right)$$

Υπενθυμίζεται ότι για $z\to\infty$, $\sum_{z\geq 1}^{\infty} Q(z,z) = 1 - \frac{1}{12z} + \frac{1}{288z^2} + \frac{139}{51840z^3} - \frac{571}{24883200z^4} + o((\frac{1}{z})^5$

$$\lim_{z\to\infty} Q(z,z) = \frac{1}{2}\lim_{z\to\infty}(1 - \frac{1}{12z} + \frac{1}{288z^2} + \frac{139}{51840z^3} - \frac{571}{24883200z^4} + o((\frac{1}{z})^5) \cong \frac{1}{2}\ .$$

Ένα αποτέλεσμα που προκύπτει εύκολα από την χρήση του Mathematica.

Στη συνέχεια,

$$\frac{1}{2} - Q(z,z) = \frac{1}{2} - \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o\left(z^{-\frac{1}{2}}\right)\right)}{(z-1)!} \Leftrightarrow$$

$$\frac{1}{2} - Q(z,z) = \frac{1}{2} - \frac{1}{2}\frac{\sqrt{2\pi z}\left(\frac{z}{e}\right)^{z}}{z!}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o\left(z^{-\frac{1}{2}}\right)\right) \Leftrightarrow$$

$$\frac{1}{2} - Q(z,z) = \frac{1}{2} - \frac{1}{2}\frac{\sqrt{2\pi z}\left(\frac{z}{e}\right)^{z}}{\sqrt{2\pi z}\left(\frac{z}{e}\right)^{z}\left(1 + \frac{1}{12z} + o(z^{-1})\right)}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o\left(z^{-\frac{1}{2}}\right)\right) \Leftrightarrow$$

$$\frac{1}{2}-Q(z,z)=\frac{1}{2}-\frac{1}{2}\left(1+\frac{1}{12z}+o(z^{-1})\right)\left(1-\frac{1}{3}\sqrt{\frac{2}{\pi z}}+o\left(z^{-\frac{1}{2}}\right)\right)\Leftrightarrow$$

$$\frac{1}{2}-Q(z,z)=\frac{1}{3\sqrt{2\pi z}}+o(z^{-\frac{1}{2}})$$

■

c) Για $\lambda>1, Q(z,\lambda z)\sim\frac{1}{\lambda-1}\frac{1}{\sqrt{2\pi z}}e^{-z(\lambda-1-log\lambda)}$

(Απόδειξη): Από το θεωρητικό υπόβαθρο έχω:

$$Q(z,\lambda z)=\frac{\Gamma(z,\lambda z)}{\Gamma(z)}\sim\frac{(\lambda z)^z e^{-(z\lambda)}}{z!\,(\lambda-1)}\sim\frac{1}{\lambda-1}\frac{1}{\sqrt{2\pi z}}e^{-z(\lambda-1-log\lambda)}$$

<u>Παρατήρηση</u>: Για $x>0$ θέτουμε $c(x)=x-1-logx>0$. Επίσης γνωρίζουμε $\lambda=\frac{q}{p}\in(0,1)$.

<u>Πρόταση</u>: Για $z\to\infty$, έχουμε:

$$P_{SN}(z)\sim\frac{e^{-(zc(\lambda))}}{2}.$$

<u>Απόδειξη</u>:

Από προηγούμενο θεώρημα γνωρίζω:

$$P(z,\kappa)=1-Q\left(z,\frac{\kappa zp}{p}\right)+\left(\frac{q}{p}\right)^z e^{\frac{\kappa z(p-q)}{p}}Q(z,\kappa z)$$

Τώρα από το προηγούμενο λήμμα και συγκεκριμένα από τις σχέσεις (a),(b):

Από το (a):

$$1-Q\left(z,\frac{\kappa zq}{p}\right)\sim\frac{1}{1-\frac{\kappa q}{p}}\frac{1}{\sqrt{2\pi z}}e^{-z\left(\frac{\kappa q}{p}-1-\log\left(\frac{\kappa q}{p}\right)\right)}\overset{\kappa=1}{\Longrightarrow}\frac{1}{1-\frac{q}{p}}\frac{1}{\sqrt{2\pi z}}e^{-\left(\frac{q}{p}-1-\frac{\log q}{p}\right)}\Leftrightarrow$$

$$1-Q\left(z,\frac{\kappa zq}{p}\right)=\frac{1}{1-\frac{q}{p}}\frac{1}{\sqrt{2\pi z}}e^{-zc\left(\frac{q}{p}\right)}\Leftrightarrow$$

$$1-Q\left(z,\frac{\kappa zq}{p}\right)=o\left(e^{-zc\left(\frac{q}{p}\right)}\right).$$

Από το (b) για $\kappa=1$:

$$\left(\frac{q}{p}\right)^z e^{\frac{\kappa z(p-q)}{p}} Q(z,\kappa z) = \left(\frac{q}{p}\right)^z e^{\kappa z\left(\frac{p-q}{q}\right)} Q(z,\kappa z) = e^{-z\left(\frac{q}{p}-1-\frac{\log p}{q}\right)} \frac{z^{z-1}\sqrt{\frac{\pi z}{2}}}{(z-1)!} \Leftrightarrow$$

$$e^{-zc\left(\frac{q}{p}\right)} \frac{z^{z-1}\sqrt{\frac{\pi z}{2}}}{(z-1)!}, \text{όπου } \frac{z^{z-1}\sqrt{\frac{\pi z}{2}}}{(z-1)!} \sim \frac{1}{2} \Leftrightarrow$$

Όποτε:

$$\left(\frac{q}{p}\right)^z e^{\frac{z(p-q)}{p}} Q(z,z) \cong \frac{1}{2} e^{-zc\left(\frac{q}{p}\right)}.$$

■

Λόγω $c(x) = x - 1 - logx$ και $\frac{1}{1-\frac{q}{p}} \frac{1}{\sqrt{2\pi z}} \sim 1$!

ΚΕΦΑΛΑΙΑ 3-4 Μαθηματικό υπόβαθρο ECDSA

3.1 Το πρόβλημα του διακριτού λογαρίθμου:

Από τα σημαντικότερα μαθηματικά προβλήματα πάνω στο οποίο στηρίχθηκαν σπουδαίες εφαρμογές στο χώρο της κρυπτογραφίας και που αποτέλεσε πρόδρομο για μελλοντικές μελέτες των περισσότερων διακριτών λογαριθμικών εργαλείων όπως το ECDSA είναι το πρόβλημα διακριτού λογαρίθμου DLP το οποίο αναφέρεται ως εξής:

Το πρόβλημα διακριτού Λογαρίθμου - Discrete Logarithmic Problem

Έστω μια ομάδα G και στοιχείο g, με $g \in G$. Τότε για γνωστό στοιχείο h της παραγόμενης από το g υποομάδας της αρχικής G, έστω SG αναζητούμε ακέραιο αριθμό m, τέτοιον ώστε:

$$h = g^m$$

Ο μικρότερος αριθμός m, που ικανοποιεί την παραπάνω σχέση ονομάζεται λογάριθμος του h σε σχέση με το g, δηλαδή $m = \log_g(h)$.

Γενικά ομάδα ονομάζουμε μια αλγεβρική δομή που αποτελείται από αριθμούς εφοδιασμένους με μία πράξη, όπως η πρόσθεση, η οποία συνδέει δύο από αυτούς και παράγει ένα τρίτο. Ο νέος αυτός αριθμός ικανοποιεί τέσσερις αξιωματικές ιδιότητες που αναφέρονται καλύτερα σε επόμενη ενότητα.

Συχνές εφαρμογές του παραπάνω θεωρητικού προβλήματος είναι συστήματα παραγωγής και επικύρωσης ψηφιακών μηνυμάτων όπως το Diffie-Hellman(DH) και EL Gamal, οι γεννήτριες ψευδοτυχαίων αριθμών και μεταβλητών και οι αλγόριθμοι παραγοντοποίησης πολλαπλασιασμού Lenstra σε ελλειπτικές καμπύλες(Lenstra elliptic-curve factorization).

Όμως παρά την ευρύτατη χρήση του είναι αντικειμενικά ένα δύσκολο πρόβλημα, γεγονός που κάνει απαραίτητη την επιστράτευση ισχυρών υπολογιστικών συστημάτων με σκοπό την επίλυση του. Γενικά για ευκλείδειους λογαρίθμους σε ομάδες $\mathbb{Z} / m\mathbb{Z}$, με πράξη την πρόσθεση ή για αναλυτικούς πάνω στις $\mathbb{R}^*$ ή $\mathbb{C}^*$ με πράξη των πολλαπλασιασμό είναι εύκολη η επίλυση του προβλήματος. Αντίθετα για πεπερασμένες ομάδες F_p^* με πράξη τον πολλαπλασιασμό (η ανάλυση των οποίων γίνεται σε επόμενη ενότητα), ο χρόνος επίλυσης αυξάνεται κατά πολύ.

Στόχος της εργασίας δεν είναι η ανάλυση του συγκεκριμένου προβλήματος αλλά η εκτενής ανάλυση των μαθηματικών εννοιών και η ανάδραση αυτών που στηρίζουν την θεωρία του διακριτού λογαριθμικού προβλήματος ελλειπτικών καμπυλών ECDLP. Παρόλα αυτά μια αναφορά σε αυτό είναι απαραίτητη από την στιγμή που εννοιολογικά στηριζόμαστε σε ένα πολύ μεγάλο βαθμό σε αυτό.

3.2 Θεωρία ελλειπτικών καμπυλών

(Εισαγωγή): Μια ελλειπτική καμπύλη πέρα από καμπύλη είναι μια ομάδα σημείων η οποία προσδιορίζεται γεωμετρικά. Τα σημεία που την απαρτίζουν έχουν συντεταγμένες σε σύνολα όπως Q, R και C. Το πρόβλημα που θα μελετήσουμε σε επόμενο κεφάλαιο είναι η εύρεση διακριτών λογαρίθμων σε ομάδες σημείων πάνω σε ελλειπτικές καμπύλες που διαγράφονται πάνω σε συγκεκριμένο πεδίο Galois, ευρύτερα γνωστό ως πρόβλημα διακριτού λογαρίθμου σε ελλειπτικές καμπύλες (ECDLP). Στη συγκεκριμένη ενότητα αφιερώνουμε χρόνο στην αποσαφήνιση των βασικών εννοιών, μορφών και θεωρημάτων που στηρίζουν την θεωρία ελλειπτικών καμπυλών που εφαρμόζονται πάνω σε πεδία Galois.

(Μορφή): Ελλειπτική, ονομάζουμε μια καμπύλη η μορφή της οποίας δίνεται από την εξίσωση:

$$y^2 = x^3 + Ax + B, \text{όπου } A, B \in \mathbb{Z}$$

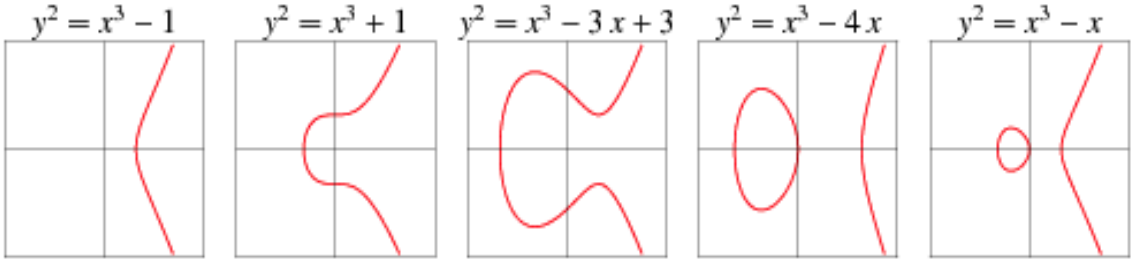
Όπου βασική προϋπόθεση είναι:

$$\Delta = 4A^3 + 27B^2 \neq 0$$

Τα σημεία της γενικότερα δίνονται από το σύνολο:

$$E = \{(x, y): y^2 = x^3 + Ax + B\} \cup \{O\},$$ όπου O ονομάζουμε το σημείο-άπειρο.

Σχηματικά παραδείγματα:

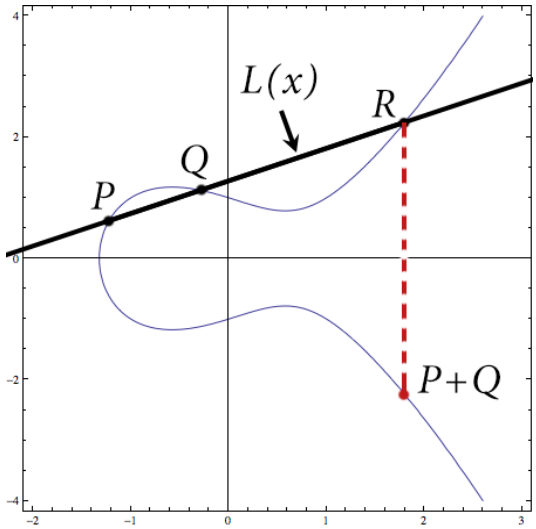


<u>Περίπτωση 1-(Point Addition)</u>: Μια από τις βασικές ιδιότητες στις ελλειπτικές καμπύλες είναι εκείνη της πρόσθεσης σημείων (Point addition). Συγκεκριμένα η μεθοδολογία είναι η εξής:

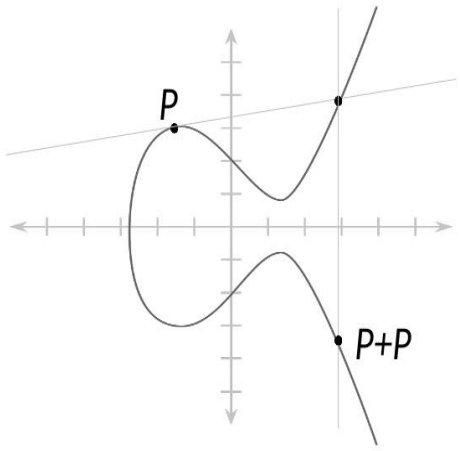
1. Πάνω σε ελλειπτική καμπύλη E επιλέγω δύο τυχαία σημεία P, Q.
2. Διαγράφω την ευθεία, έστω L που ενώνει τα σημεία μου.
3. Ονομάζω το τρίτο σημείο στο οποίο η L, τέμνει την E έστω R.
4. Φέρνω κάθετη από το τρίτο σημείο ως προς τον οριζόντιο άξονα στο επίπεδο.
5. Το νέο σημείο, έστω R', είναι η ανάκλαση του σημείου R και είναι το αλγεβρικό άθροισμα των αρχικών P, Q.

Περίπτωση 2-(Point doubling): Αν αρχικά είχαμε μόνο αρχικό σημείο P, τότε φέρνω την εφαπτομένη L από το σημείο αυτό η οποία με την σειρά της τέμνει την ελλειπτική καμπύλη σε ένα δεύτερο σημείο R του οποίου η ανάκλαση ως προς τον οριζόντιο άξονα είναι ίσης με $2P$.

Σχηματικά έχω:



Παράδειγμα Point Adding



Παράδειγμα Point Doubling

(Απόδειξη Point Addition): Για δοσμένη ελλειπτική καμπύλη E, αρχικά σημεία P_1, P_2 όπου $P_1(x_1, y_1)$ & $P_2(x_2, y_2)$ φέρουμε ευθεία L, η οποία τέμνει την καμπύλη σε σημείο $P_3(x_3, y_3)$ και αναμένουμε ανάκλαση $P_3'(x_3, y_3)$.

Η εξίσωση της ευθείας δίνεται ως εξής:

$$y - y_1 = \lambda(x - x_1) \Leftrightarrow$$

$$y - y_1 = \lambda x - \lambda x_1 \Leftrightarrow$$

$$y = \lambda x + \{y_1 - \lambda x_1\}, \text{ και θέτω } \beta = -\lambda x_1 + y_1 \Leftrightarrow$$

$$y = \lambda x + \beta.$$

Υπενθυμίζεται ότι η κλίση της ευθείας υπολογίζεται $\lambda = \frac{y-y_1}{x-x_1}$.

Από την ειδικότερη εξίσωση $y^2 = x^3 + ax + b$ των ελλειπτικών καμπυλών δεδομένου του λ προκύπτει:

$$(\lambda x + \beta)^2 = x^3 + \alpha x + b \Leftrightarrow$$

$$\lambda^2 x^2 + \beta^2 + 2\beta \cdot \lambda x = x^3 + ax + b \Leftrightarrow$$

$x^3 - \lambda^2 x^2 + (a - 2\beta \cdot \lambda)x + (b - \beta^2) = 0$, μια εξίσωση $3^{ου}$ βαθμού.

Για $\lambda^2 = x_1 + x_2 + x_3 \Rightarrow x_3 = \lambda^2 - x_1 - x_2$, οπότε για το σημείο P_3', θα έχουμε:

$$y_3' = \lambda x_3 + \beta, \text{όπου } x_3 \text{ γνωστό}$$

$$y_3' = \lambda x_3 + y_1 - \lambda x_1 \Leftrightarrow$$

$$y_3' = \lambda(x_3 - x_1) + y_1$$

Παρατηρώ όμως βάσει των παραπάνω ότι:

$$y_3 = \lambda x_3 + \beta \Leftrightarrow y_3 = \lambda x_3 + (-\lambda x_1 + y_1) \Leftrightarrow y_3 = \lambda(x_1 - x_3) - y_1 \equiv {y_3}'$$

■

(Απόδειξη του Point Doubling): Από τα προηγούμενα, έχω $y_3 = \lambda(x_1 - x_3) - y_1$. Από την στιγμή όμως που $x_1 = x_2$, έχω:

$$x_3 = \lambda^2 - 2x_1 \ \& \ y_3 = \lambda(x_1 - x_3) - y_1$$

Βέβαια τώρα για την εύρεση της κλίσης λ, έχω:

$$y^2 = x^3 + ax + b \ \kappa\alpha\iota \ \alpha\nu \ f(x) = x^3 + ax + b \ \tau\acute{o}\tau\varepsilon:$$

$y = \sqrt{f(x)}$, άρα:

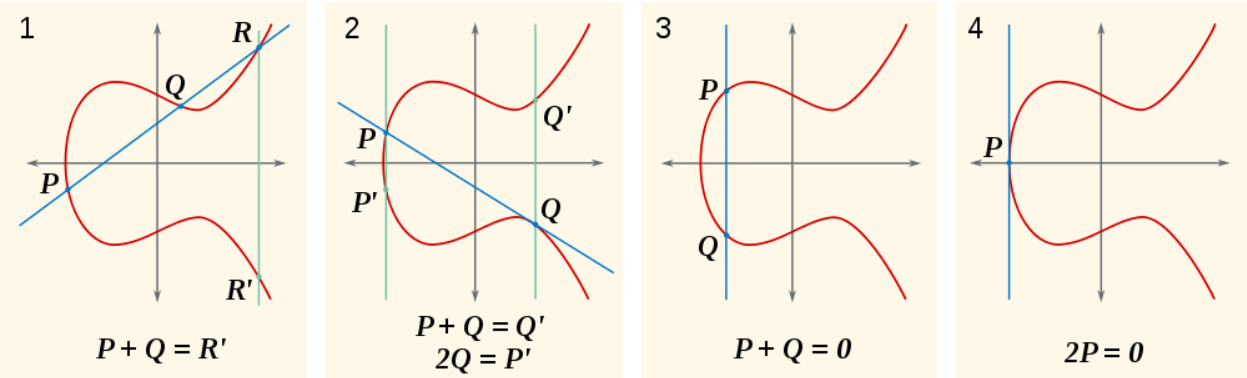
$$\lambda = \frac{dy}{dx} = \frac{d(\sqrt{f(x)}}{df(x)} \cdot \frac{df(x)}{dx}, \text{ χρήση του κανόνα αλυσίδας!}$$

Τότε:

$$\lambda = \frac{1}{2\sqrt{f(x)}} \cdot \frac{d(x^3+ax+b)}{dx} = \frac{1}{2y} \cdot (3x^2 + a), \text{ άρα τελικά } \lambda = \frac{3x^2+a}{2y}$$

■

<u>*Περίπτωση 3(Νοητό σημείο προς το άπειρο)*</u>: Για αρχικό σημείο $P \in E$, επιλέγω το $Q = -P$, τότε η κάθετη γραμμή που τα συνδέει τείνει προς το άπειρο και δεν τέμνει την καμπύλη σε κανένα σημείο. Το νοητό O είναι ο γεωμετρικός τόπος όλων των σημείων της καθέτου (Διάγραμμα 3).



Θεώρημα(Γενικές Ιδιότητες): Στη περίπτωση της προσθήκης σημείου (point addition) ισχύουν συγκεκριμένες αλγεβρικές ιδιότητες που παρατηρούνται όταν εφαρμόζεται σε δεδομένη ελλειπτική καμπύλη E. Για αρχικά σημεία $P, Q, R \in E$ ισχύουν τα εξής:

i. $P + 0 = 0 + P = P$
ii. $P + (-P) = 0$
iii. $P + (Q + R) = (P + Q) + R$
iv. $P + Q = Q + P$

Θεώρημα(Αλγεβρικές ιδιότητες): Όπως και πριν για δύο σημεία $P_1 = (x_1, y_1)$ και $P_2 = (x_2, y_2)$ πάνω σε ελλειπτική καμπύλη της μορφής $E: y^2 = x^3 + Ax + B$, τότε ισχύουν οι παρακάτω ιδιότητες:

- Εάν έχω $P_1 \neq P_2$ με $x_1 = x_2$, τότε $P_1 + P_2 = 0$.
- Εάν $P_1 = P_2$ και $y_1 = 0$, τότε $P_1 + P_2 = 2P_1 = 0$.
- Εάν $P_1 \neq P_2$ και $x_1 \neq x_2$, τότε $\begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} \\ \beta = -\lambda x_1 + y_1 = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{cases}$
- Εάν $P_1 = P_2$ με $y_1 \neq 0$, τότε $\begin{cases} \lambda = \frac{3x_1^2 + A}{2y_1} \\ \beta = -\lambda x_1 + y_1 = \frac{-x^3 + Ax + 2B}{2y} \end{cases}$
- Ισχύει από τα προηγούμενα ότι σε γενικές γραμμές:

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \beta$$

Στο επόμενο κεφάλαιο αναφερόμαστε στη θεωρεία των πεπερασμένων πεδίων Galois, η οποία σε συνδυασμό με την παραπάνω ανάλυση οδήγησαν μαθηματικούς όπως τον Poincare να αποδείξουν θεωρήματα, όπως το παρακάτω:

Θεώρημα Poincare: Για πεδίο τιμών F και δεδομένη ελλειπτική καμπύλη $E: y^2 = x^3 + Ax + B$ $με$ $A, B \in F$. Τότε συμβολίζουμε $E(F)$ το σύνολο των σημείων της καμπύλης με συντεταγμένες στο πεδίο F, δηλαδή $E(F) \coloneqq \{(x, y) \in E: x, y \in F\} \cup \{O\}$.

Όπου τότε το $E(F)$ αποτελεί υποσύνολο του συνόλου των σημείων της καμπύλης E.

3.3 Πεδία Galois(Πεπερασμένα πεδία) & χαρακτηριστικές ιδιότητες

Τα πεδία Galois είναι η δεύτερη μαθηματική θεωρία η οποία σε συνδυασμό με τις ελλειπτικές καμπύλες στηρίζει το διακριτό λογαριθμικό πρόβλημα ελλειπτικών καμπυλών (ECDLP) πάνω στο οποίο στηρίζεται αλγοριθμικά η πλατφόρμα του Bitcoin.

Είναι βασικό να γνωρίζει κανείς τί είναι πεδίο. Πεδίο ονομάζουμε ένα σύνολο στοιχείων-αριθμών, έστω F, εφοδιασμένο με τις πράξεις της πρόσθεσης (+) και του πολλαπλασιασμού(*),

για την οποία ισχύουν οι αξιωματικές ιδιότητες τους. Οι αξιωματικές ιδιότητες των παραπάνω πράξεων είναι:

Όνομα Ιδιότητας	Πρόσθεση	Πολλαπλασιασμός
Αντιμεταθετική	$a + b = b + a$	$a \cdot b = b \cdot a$
Προσεταιριστική	$(a + b) + c = a + (b + c)$	$(a \cdot (b) \cdot c) = a \cdot (b \cdot c)$
Επιμεριστική	$a \cdot (b + c) = a \cdot b + a \cdot c$	$(a + b) \cdot c = a \cdot c + b \cdot c$
Ουδέτερο Στοιχείο	$a + 0 = 0 + a = 0$	$a \cdot 1 = 1 \cdot a = a$
Αντίθετο Στοιχείο	$a + (-a) = (-a) + a = 0$	$a \cdot a^{-1} = a^{-1} \cdot a = 1, για\ α \neq 0$

Ο αριθμός των στοιχείων του πεδίου αποτελούν την τάξη (order) του πεδίου, η οποία είναι είτε πρώτος αριθμός είτε δύναμη πρώτου(binary fields).

Βασική ομάδα των πεδίων είναι τα πρωτεύοντα πεδία(prime fields), των οποίων η τάξη είναι πρώτος αριθμός. Για κάθε πρωτεύουσα δύναμη p, υπάρχει ακριβώς ένα (με τη συνήθη επιφύλαξη ότι "ακριβώς ένα" σημαίνει "ακριβώς ένα μέχρι έναν ισομορφισμό") πεπερασμένο πεδίο $GF(p)$, όπου γράφεται επίσης και F_{p^n}.

Παρατήρηση: Συμβολίζουμε $GF()$ το πρωτεύων πεδίο της τάξης () που περιλαμβάνει τα υπόλοιπα των διαιρέσεων των στοιχείων με την πράξη-modulo p, συνεπώς τα στοιχεία του πεδίου είναι τα $\{0,1,2, \dots, p-1\}$. Για τον λόγο αυτό είναι καλύτερο να το συμβολίζονται ως $GF(p^n)$ αντί για $GF(k)$, όπου $k = p^n$.

3.3.1 Θεωρητικό υπόβαθρο των πεδίων Galois

Για να μπορέσει να κατανοήσει κάποιος την έννοια του πεδίου πρέπει πρώτα να έρθει σε επαφή με προγενέστερες δομές όπως είναι η ομάδα και ο δακτύλιος. Παρακάτω παρουσιάζονται συνοπτικά τα βασικά χαρακτηριστικά των παραπάνω δομών.

Ορισμός(Ομάδα): Ομάδα ονομάζεται ένα σύνολο σημείων, έστω G εφοδιασμένο με μία δυαδική πράξη $*$, για το οποίο ισχύουν οι εξής ιδιότητες:

- (Προσεταιριστική ιδιότητα): Για $a, b, c \in G$, ισχύει $a * (b * c) = (a * b) * c$
- (Ταυτοτικό Στοιχείο): Υπάρχει στοιχείο $e, e \in G$ ώστε $\forall\ a \in G$, ισχύει $a * e = e * a = a$.
- (Αντίστροφο Στοιχείο): Για $a \in G$, υπάρχει $a^{-1} \in G$, ώστε $a * a^{-1} = a^{-1} * a = e$.

Επιπλέον αν:

- $\forall\, a, b\ \in G$ με $a * b = b * a$ η ομάδα είναι αβελιανή-αντιμεταθετική (abelian-commutative)

Παρατήρηση: Μια ομάδα καλείται πεπερασμένη όταν περιέχει πεπερασμένο αριθμό στοιχείων, το σύνολο των οποίων καλείται τάξη (order) και συμβολίζεται $n = |G|$.

Ορισμός(Κυκλική Ομάδα και στοιχείο γεννήτρια): Μια πολλαπλασιαστική ομάδα(με πράξη τον πολλαπλασιασμό) είναι κυκλική εάν:

$$\forall\, b \in G, \exists\, j \in \mathbb{N}\ με\ b = a^j$$

Το στοιχείο a είναι το στοιχείο γεννήτρια της κυκλικής ομάδας. Συμβολίζουμε $G \cong < a >$.

Ορισμός(Υποομάδα Η): Υποομάδα H, ονομάζουμε ένα υποσύνολο μιας ομάδας G που ικανοποιεί τις ίδιες ιδιότητες με την ομάδα. Η υποομάδα περιέχει το ταυτοτικό στοιχείο της G και η τάξη της είναι h, όπου h διαιρέτης της τάξης n της ομάδας.

Ορισμός (Δακτύλιος): Δακτύλιο R, ονομάζουμε ένα σύνολο αριθμών εφοδιασμένο με τις δυαδικές πράξεις $\{+,\cdot\}$, ώστε να ισχύουν:

- Το σύνολο R είναι αβελιανή ομάδα ως προς την $+$.
- Η πράξη $\cdot$ είναι προσεταιριστική, δηλαδή $\forall\, a, b, c\ \in R$, ισχύει $a \cdot (b \cdot c) = a \cdot (b \cdot c)$
- Ισχύει η επιμεριστική ιδιότητα $\forall a, b, c \in \mathbb{R}$ όπως αναφέρθηκε στην εισαγωγή.

Επιπλέον:

- Δακτύλιο με ταυτότητα ονομάζουμε ένα δακτύλιο R εφοδιασμένο με ένα πολλαπλασιαστικό ταυτοτικό στοιχείο e, όπου $a \cdot e = e \cdot a = a$.
- Ο δακτύλιος καλείται αντιμεταθετικός εάν η $\cdot$ είναι αβελιανη(ορισμός ομάδας).
- Ο δακτύλιος καλείται ακέραιη περιοχή, εάν είναι αντιμεταθετικός με ταυτοτικό στοιχείο $e, e \neq 0$.
- Ο δακτύλιος R είναι αφαιρετικός (division ring) εάν τα μη-μηδενικά στοιχεία του παράγουν ομάδα με πράξη $\cdot$.

(Παράδειγμα Δακτυλίου): Τα σύνολα $\mathbb{Z}_m$ ή $\mathbb{Z}/(m)$ που περιέχουν τα στοιχεία $\{0,1,2, \dots, m-1\}$ εφοδιασμένα με τις πράξεις $\begin{cases} +: a + b\ στον\ \mathbb{Z}_m\ = (a + b)\ mod\ m \\ \cdot: a \cdot b\ στον\ \mathbb{Z}_m = a \cdot b\ mod\ m \end{cases}$ είναι δακτύλιοι.

Θεώρημα: Κάθε πεπερασμένη ακέραια περιοχή αποτελεί πεδίο.

(Απόδειξη): Έστω πεπερασμένη ακέραια περιοχή R, με στοιχεία $a_1, a_2, \dots, a_n$. Για ένα μη μηδενικό στοιχείο $a \in R$ μπορούμε να παράγουμε τα γινόμενα $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_n$, τα οποία είναι διακριτά μεταξύ τους εφόσον αν $a \cdot a_i = a \cdot a_j$ τότε θα είχαμε $a \cdot (a_i - a_j) = 0$. Από την στιγμή που $a \neq 0$, έχω $a_i - a_j = 0 \Leftrightarrow a_i = a_j$. Οπότε κάθε στοιχείο της περιοχής έχει την μορφή $a \cdot a_i$ και φυσικά $e = a \cdot a_i$ για κάποιο $1 \leq i \leq n$, με e το ταυτοτικό στοιχείο της

περιοχής. Τώρα επειδή ο δακτύλιος είναι αντιμεταθετικός έχω $a_i \cdot a = e$ οπότε το a_i είναι το πολλαπλασιαστικό αντίστροφο στοιχείο του a. Οπότε τα μη μηδενικά στοιχεία της R παράγουν μια αντιμεταθετική ομάδα που είναι ουσιαστικά πεδίο.

Παρατήρηση: Βάσει των παραπάνω πεδίο ονομάζουμε ένα αφαιρετικό αντιμεταθετικό δακτύλιο ή αλλιώς κάθε πεπερασμένη ακέραιη περιοχή ονομάζεται δακτύλιος.

Ορισμός (Υποδακτύλιος): ονομάζουμε ένα δακτύλιο S, όλα τα στοιχεία του οποίου ανήκουν σε αρχικό δακτύλιο R, με την προϋπόθεση ότι τα αποτελέσματα των δυαδικών πράξεων $+,\cdot$ περιορίζονται στον ίδιο τον υποδακτύλιο. Συμβολίζεται με $(S, +, \cdot, 0, 1)\ με\ S \subseteq R$.

Θεώρημα: Ο $\mathbb{Z}/(p)$ ο δακτύλιος των υπολοίπων των κλάσεων των ακεραίων με πράξη modulo με ένα αριθμό n που παράγεται από τον πρώτο αριθμό p, αποτελεί ένα πεδίο.

(Απόδειξη): Αρκεί να αποδείξουμε ότι ο δακτύλιος $\mathbb{Z}/(p)$ είναι ακέραια περιοχή. Γνωρίζω ότι το 1 είναι ταυτοτικό στοιχείο του δακτυλίου και επίσης ισχύει η ιδιότητα $[a][b] = [ab] = [0]$ εάν και μόνο αν ισχύει $a \cdot b = k \cdot p$, για k. Όμως λόγω ότι p είναι πρώτος αριθμός, τότε ο p διαιρεί το $a \cdot b$ μόνο αν διαιρεί ένα τουλάχιστο από τους δύο παράγοντες. Αναγκαστικά είτε $[a] = 0$ ή $[b] = 0$, αρά είναι εμφανές ότι ο δακτύλιος δεν περιέχει κανένα μηδενικό διαιρετή.

Ορισμός (Χαρτογράφηση φ): χαρτογράφηση $\varphi: Z(p) \to F_p$ ονομάζουμε ένα ισομορφισμό, τέτοιο ώστε να ισχύουν οι ιδιότητες:

$$\varphi([a] + [b]) = \varphi([a]) + \varphi([b]) \ \ \& \ \varphi([a][b]) = \varphi([a]) \cdot \varphi([b]).$$

Το πεπερασμένο πεδίο F_p έχει μηδενικό στοιχείο 0 και ταυτοτικό 1 και παρόμοια δομή με τον δακτύλιο $Z/(p)$.

Παρατήρηση: για οποιαδήποτε δύο στοιχεία του πεδίου εκτελέσουμε που πρόσθεση ή πολλαπλασιασμό, το αποτέλεσμα θα ανήκει στο πεδίο (χαρακτηριστικό των πεπερασμένων ομάδων).

Ορισμός (Πεδίο Galois): Για ένα πρώτο αριθμό p, όπου F_p είναι το σύνολο {0,1,…,p-1} των αντίστοιχων ακεραίων και έστω $\varphi: Z(p) \to F_p$ η χαρτογράφηση που ορίζεται από το $\varphi([\alpha]) = \alpha$, όπου $a = 0,1, \dots, p-1$. Τότε το $F(p)$, ορισμένο με την βασική δομή των πεδίων και την χαρτογράφηση φ, είναι ένα πεπερασμένο πεδίο, γνωστότερα ως πεδίο Galois τάξεως p.

Όταν χρησιμοποιούμε την πράξη $a\ (mod\ m) = b$, το b είναι το υπόλοιπο του a διαιρεμένο με την ποσότητα m, όπου για $a = m \cdot q + b$. Τέλος το b προσδιορίζεται κατά μοναδικό τρόπο από τα a, m.

(Παράδειγμα): Τα στοιχεία του πεδίου Galois F_{29} είναι $\{0,1,2,3, \dots ,28\}$. Παραδείγματα των αριθμητικών πράξεων είναι τα:

- Πρόσθεση: 17+20=8, διότι 37 mod 29 = 8

- Πολλαπλασιασμός: 17-20=26, λόγω -3 mod 29 = 26
- Πολλαπλασιασμός: 17*20=21, διότι 340 mod 29 = 21
- Διαίρεση: 17^{-1}=12, λόγω 17*12 mod 29 = 1

Ορισμός(Χαρακτηριστικό πεδίου): Για αρχικό πεδίο F με τάξη q πρώτο αριθμό για τον οποίο ισχύει $q = p^m$ με p επίσης πρώτο και m θετικό ακέραιο, τότε το p ονομάζεται χαρακτηριστικό του πεδίου. Σε περίπτωση που δεν υπάρχει τέτοιος ακέραιος το χαρακτηριστικό είναι το 0.

Θεώρημα: Ένα πεπερασμένο πεδίο έχει χαρακτηριστικό που είναι πρώτος αριθμός ή 0.

(Εναλλακτικός ορισμός χαρακτηριστικού πεδίου): Για αρχικό πεδίο F, ο μικρότερος θετικός ακέραιος p, τέτοιος ώστε $p * 1 = 0$, Σε περίπτωση που δεν υπάρχει τέτοιος ακέραιος το χαρακτηριστικό είναι το 0.

(Απόδειξη): Καταρχήν το 1 δεν θα μπορούσε να είναι χαρακτηριστικό από την στιγμή που γνωρίζω ότι $1 \cdot 1 \neq 0$. Έστω ότι το χαρακτηριστικό p του πεδίου F δεν είναι πρώτος αριθμός. Τότε $p = m * n, όπου\ m < p\ \&\ n > 1$. Όποτε:

$$p \cdot 1 = 0 \Leftrightarrow$$

$$(m \cdot n) * 1 = 0 \Leftrightarrow$$

$$\left(\sum_{i-1}^{m} 1\right) \cdot \left(\sum_{i=1}^{n} 1\right) = 0 \Leftrightarrow$$

$(m \cdot 1) * (n \cdot 1) = 0 \Leftrightarrow \begin{cases} m \cdot 1 = 0 \\ n \cdot 1 = 0 \end{cases}$, το οποίο είναι αδύνατο λόγω των υποθέσεων.

Άρα το χαρακτηριστικό είναι πάντοτε πρώτος αριθμός.

Παρατήρηση: Τα πολλαπλάσια της ταυτότητας έστω e, είναι $e, 2e, 3e\ κτλ$. Από την στιγμή που το πεδίο έχει πεπερασμένο αριθμό στοιχείων, τότε θα υπάρχουν ακέραιοι $k, m\ ώστε\ 1 \leq k \leq m$ ώστε $\begin{cases} k \cdot e = m \cdot e \\ (m-k) \cdot e = 0 \end{cases}$ οπότε το πεδίο έχει θετικό χαρακτηριστικό.

Ορισμός (Υποπεδίο-Επέκταση πεδίου): Για πεδίο F, ονομάζουμε K ένα υποπεδίο του, όταν αυτό είναι επίσης πεδίο εφοδιασμένο με τις ίδιες πράξεις όλα τα στοιχεία του οποίου ανήκουν στο αρχικό F. Κατ' αναλογία το F αποτελεί επέκταση του υποπεδίου K.

Ορισμός (Πρωτεύον Πεδίο): Εάν ένα πεδίο δεν περιέχει υποπεδία, ονομάζεται πρωτεύον πεδίο. Γενικά ένα πεδίο με τάξη πρώτο αριθμό είναι πρωτεύον.

Παρατήρηση: Εάν το K είναι υποπεδίο ενός πεπερασμένου πρωτεύοντος F_p (p πρώτος), τότε πρέπει να περιέχει τα στοιχεία 0,1 του F_p. Επιπλέον ένα πεπερασμένο πεδίο F_{p^m} έχει ένα υποπεδίο τάξεως p^l για κάθε θετικό διαιρέτη l του m. Τα στοιχεία του υποπεδίου K είναι τα a, όπου $\forall\ a\ \in F_{p^m}$ ικανοποιείται η σχέση σχέση $a^{p^l} = a$.

Ορισμός (Στοιχείο Γεννήτρια): Ένα στοιχείο $a \in F_q$, όπου F_q πεδίο ονομάζεται στοιχείο γεννήτρια του πεδίου όταν ισχύει:

$$F_q = \{0, a, a^2, a^3, \dots, a^{q-1}\}.$$

Ορισμός (Βάση πεδίου Galois): Αλγεβρικά ένα πεπερασμένο πεδίο F_{p^n} μπορεί να αποτελέσει ένα διανυσματικό χώρο του υποπεδίου του F_p, όπου τα διανύσματα θα είναι τα στοιχεία του πρώτου και βαθμωτά μεγέθη τα στοιχεία του δεύτερου, ανάλογα βέβαια την πράξη που χρησιμοποιούμε. Για $B = \{b_1, b_2, \dots, b_n\}$ μια βάση και $a \in F_{p^n}$, τότε το στοιχείο του πεδίου μπορεί να παραστεί κατά μοναδικό ως $a = a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots + a_n \cdot b_n$ με $(a_1, a_2, \dots, a_n)$ στοιχεία του F_p.

Ορισμός(Πολλαπλασιαστική Ομάδα πεδίου *F*): Η πολλαπλασιαστική ομάδα, είναι μία ομάδα με πράξη τον πολλαπλασιασμό των μη μηδενικών αναστρέψιμων στοιχείων ενός αρχικού πεδίου F, η ιδιότητα της οποίας αναφέρεται ως πολλαπλασιασμός. Συμβολίζεται με F_q^*.

(Παράδειγμα): Στην περίπτωση ενός πεδίου F, η ομάδα είναι $(F \setminus \{0\}, \bullet)$, όπου 0 αναφέρεται στο μηδενικό στοιχείο του F και η δυαδική λειτουργία • είναι ο πολλαπλασιασμός πεδίου.

3.3.2 Χαρακτηριστικές ιδιότητες πεδίων Galois

Έχοντας πλέον αποσαφηνίσει τις βασικές έννοιες των πεπερασμένων πεδίων προχωράμε σε ιδιότητες και χαρακτηριστικά που αποτελούν θεωρητικό υπόβαθρο των επόμενων κεφαλαίων.

Λήμμα: Για F ένα πεπερασμένο πεδίο με χαρακτηριστικό p το πεδίο έχει p^m στοιχεία με το m, να είναι $m \geq 1$.

(Απόδειξη): Για ένα τυχαίο στοιχείο $a_1 \in F$. Τότε θεωρούμε ότι $0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1$ είναι ανά δύο διαφορετικά. Εάν ισχύει $a_1 \cdot i = a_1 \cdot j \; \gamma\iota\alpha \; 0 \leq i \leq j \leq p-1$ τότε $(j-i) \cdot a_1 = 0$. Οπότε αναγκαστικά $i = j$ και αν $F = \{0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1\}$ η απόδειξη τελειώνει. Εναλλακτικά επιλέγουμε $a_2 \in F \setminus \{0 \cdot a_1, 1 \cdot a_1, \dots, (p-1) \cdot a_1\}$. Θεωρούμε ότι είναι ανά δύο διαφορετικά. Εάν ισχύει:

$$c_1 \cdot a_1 + c_2 \cdot a_2 = b_1 \cdot a_1 + b_2 \cdot a_2 \; \gamma\iota\alpha \; 0 \leq c_1, c_2, b_1, b_2 \leq p-1, \text{ τότε } a_2 = b_2.$$

Σε αντίθετη περίπτωση $a_2 = (b_2 - c_2)^{-1} \cdot (c_1 - b_1) \cdot a_1$ θα ερχόταν σε αντίθεση με την επιλογή του a_2. Οπότε, λόγω $c_2 = b_2$, τότε $c_1 = b_1$.

Παρατήρηση: Στην πολυωνυμική παράσταση $c_1 \cdot a_1 + c_2 \cdot a_2 + \cdots + c_n a_n$ οι όροι είναι ανά δύο διαφορετικοί $\forall \; c_i \in Z/(p)$. Επομένως $|F| = p^n$.

Λήμμα: Για τυχαίο στοιχείο b ενός πεπερασμένου πεδίου (Galois), έστω F_q με σύνολο στοιχείων q, ισχύει $b^q = b$.

(Απόδειξη): Για την τετριμμένη περίπτωση $b = 0$, προφανώς $b^q = 0 = b(mod\ b)$. Εάν $b \neq 0$ θεωρώ πεδίο $F' = \{a_1, a_2, \dots, a_{q-1}\}$. Από την θεωρεία μια άλλη έκφραση του F', είναι:

$$F' = \{b \cdot a_1, b \cdot a_2, \dots, b \cdot a_{q-1}\}, \text{ άρα λόγω:}$$

$$(b \cdot a_1) * (b \cdot a_2) * \dots * (b \cdot a_{q-1}) = b^{q-1} * (a_1 \cdot a_2 \cdot \dots \cdot a_{q-1}) = a_1 \cdot a_2 \cdot \dots \cdot a_{q-1}$$

Ως εκ τούτου $b^{q-1} = 1\ και\ b^q = b$.

Λήμμα: Για K ένα υποπεδίο ενός αρχικού πεδίου F_q, με $|F| = q$ αριθμό στοιχείων, ένα τυχαίο στοιχείο b του πεδίου ανήκει στο υποπεδίο αν και μόνο αν $b^q = b$.

(Απόδειξη):

- Το ευθύ αποδεικνύεται άμεσα από το παραπάνω λήμμα.
- (Αντίστροφο) Για πολυωνυμική παράσταση $x^q - x$, έχω μέγιστο αριθμό διακριτών ριζών q στο πεδίο F. Τώρα από την στιγμή που όλα τα στοιχεία του K είναι ρίζες της ίδιας πολυωνυμικής με $|K| = q$, μπορούμε να πούμε $K = \{\ ρίζες\ της\ x^q - x\ στο\ F\}$. Ως εκ τούτου κάθε στοιχείο $b \in F$ που ικανοποιεί την σχέση $b^q = b$ είναι και ρίζα της πολυωνυμικής $x^q - x$, οπότε $b \in K$.

Λήμμα: Για πεπερασμένο πεδίο F το οποίο έχει q στοιχεία, τότε για κάθε $w \in F$ ισχύει η σχέση $w^q = w$.

(Απόδειξη): Η ισότητα $w^q = w$ είναι τετριμμένη στη περίπτωση που $w = 0$. Στη περίπτωση των μη μηδενικών στοιχείων q του πεδίου F σχηματίζουν μια ομάδα τάξης $q - 1$ με πράξη τον πολλαπλασιασμό. Εάν $w \neq 0$, θεωρώντας $F^* = \{a_1, a_2, \dots, a_{q-1}\}$. Πλέον θα έχω:

$$F^* = \{w \cdot a_1, w \cdot a_2, \dots, w \cdot a_{n-1}\} \Leftrightarrow$$

$$a_1 \cdot a_2 \cdot \dots \cdot a_{q-1} = (w \cdot a_1) * (w \cdot a_2) * \dots * (w \cdot a_{q-1}) \Leftrightarrow$$

Οπότε ισχύει:

$$w^{q-1} = 1\ \forall\ w \in F\ με\ w \neq 0. \text{ Συνεπώς } w^q = w.$$

Θεώρημα: Για πεπερασμένο πεδίο F με χαρακτηριστικό $p > 0$, $όπου\ a, b \in F\ και\ m \geq 0$, ισχύει:

$$(a + b)^{p^m} = a^{p^m} + b^{p^m}.$$

(Απόδειξη): Αρχικά χρησιμοποιούμε τον τύπο:

$$\binom{p}{i} = \frac{p(p-1)\dots(p-(i-1))}{1\cdot 2\cdot \dots \cdot i} = 0\ mod\ p, \forall i \in \mathbb{Z}\ με\ 0 < i < p$$

Σε συνδυασμό με το δυονυμικό θεώρημα:

$$(a+b)^p = a^p + \binom{p}{i} a^{p-1}b + \dots + \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p, όταν\ m = 1$$

Δουλεύοντας επαγωγικά για $m = 2$, καταλήγουμε στο ζητούμενο.

Ορισμοί: Βοηθητικοί ορισμοί, χρήσιμοι για τα επόμενα θεωρήματα είναι:

- Ονομάζουμε πολυωνυμικό δακτύλιο πάνω σε πεδίο F μια συνάρτηση της μορφής:
  $$F[x] = \{\sum_{i=1}^{n} a_i x^i, όπου\ \alpha_\iota \in F\ με\ n \geq 0\}.$$
- $\deg\big(f(x)\big) = n$, ονομάζουμε τον βαθμό του πολυωνύμου $f(x) = \sum_{i=1}^{n} a_i x^i$
- $\deg(0) = -\infty$
- Ένα μη μηδενικό πολυώνυμο $f(x) = \sum_{i=1}^{n} a_i x^i$ με $a_n = 1$θα έχει την μορφή:
  $$x^n + a_{n-1}x^{n-1} + \dots + c_1 x + c_0$$
- Εάν $\deg\big(f(x)\big) > 0$, τότε:
  - $f(x)$ είναι αναγώγιμο εάν υπάρχουν $g(x), h(x)$ με $\deg\big(g(x)\big) < \deg(\big(f(x)\big)$ και $\deg\big(h(x)\big) < \deg(\big(f(x)\big)$ με $f(x) = g(x)\cdot h(x)$
  - Μη αναγώγιμο σε αντίθετη περίπτωση.

Παρατήρηση: Σε γενικές γραμμές από πρωτεύοντα πεδία F_p μπορούμε να παράγουμε και άλλα πρωτεύοντα μέσα από την διαδικασία προσάρτησης των ριζών.

Διαδικασία Προσάρτησης Ριζών (Root adjunction)

Γνωρίζουμε από την θεωρεία των πεδίων το εξής:

Εάν $\boldsymbol{a}$ ένα στοιχείο ενός πεδίου F πάνω σε ένα πρωτεύον πεδίο, έστω F_p, το σύνολο των ρητών συναρτήσεων στο στοιχείο/σημείο $\boldsymbol{a}$ του οποίου οι συντελεστές ανήκουν στο πρωτεύον πεδίο είναι ένα πεδίο που παράγεται από το πρωτεύον F_p με την προσθήκη του σημείου αυτού.

1. Συντελεστές: Είναι οι σταθερές a_i που συναντώνται σε πολυωνιμικές παραστάσεις της μορφής $a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, όπου x είναι η μεταβλητή του πολυωνύμου.
2. Ρητή Συνάρτηση: Ονομάζουμε τη συνάρτηση $R(x)$ που είναι το πηλίκο δύο πολυωνυμικών παραστάσεων $P(x), Q(x)$ μορφής $R(x) = \frac{P(x)}{Q(X)}$, με $Q(x) \neq 0, \forall\ x$.

Παρατήρηση: Εάν συνάρτηση $f \in F_p[x]$ είναι μία αμείωτη πολυωνυμική σχέση πάνω στο F_p βαθμού n, μπορούμε με συγχώνευση μιας ρίζας της f στο πρωτεύον πεδίο $F_p[x]$, να λάβουμε ένα πεπερασμένο πεδίο με p^n στοιχεία.

Λήμμα: Για πεπερασμένο πεδίο F με συνολικά στοιχεία q και K ένα ύποπεδίο του F, γνωρίζω ότι η πολυωνυμική σχέση $x^q - x$ στο $K[x]$ υπολογίζεται στο $F[x]$ πεδίο ως:

$$x^q - x = \prod_{a \in F} (x - a),$$

Και το πεδίο F είναι διαχωριζόμενο πεδίο του $x^q - x$ πάνω στο υποπεδίο K.

Απόδειξη: Η πολυωνυμική παράσταση $x^q - x$ βαθμού q έχει μέγιστο αριθμό ριζών q στο πεδίο F. Βάσει του προηγουμένου λήμματος (για πεπερασμένο πεδίο F το οποίο έχει q στοιχεία, τότε για κάθε $w \in F$ ισχύει η σχέση $w^q = w$) γνωρίζουμε q τέτοιες ρίζες που είναι όλα τα στοιχεία του πεδίου. Έτσι, η παραπάνω πολυωνυμική χωρίζεται στο F με τον τρόπο που υποδεικνύεται χωρίς να μπορεί να χωριστεί σε μικρότερο πεδίο. Έτσι καταλήγουμε στο ζητούμενο.

Προχωράμε στα τελευταία θεωρήματα που είναι τα πιο ουσιώδη για την θεωρεία των πεδίων Galois.

Θεώρημα(Ύπαρξης και μοναδικότητας): Για κάθε πρώτο αριθμό p και θετικό ακέραιο n υπάρχει πεπερασμένο πεδίο με p^n στοιχεία. Οποιοδήποτε άλλο πεπερασμένο πεδίο με ίδιο αριθμό στοιχείων είναι ισομορφικό με το διαχωριζόμενο πεδίο της ποσότητας $x^q - x$ πάνω στο F_p.

(Απόδειξη Ύπαρξης): Υπενθυμίζονται τα εξής χαρακτηριστικά των πεδίων:

1. Ένα στοιχείο $l \in F$, είναι πολλαπλή ρίζα για πολυώνυμο f του πεδίου, όταν είναι ρίζα και των δύο πολυωνύμων f, f'.
2. Για τυχαίο δακτύλιο R με πρωτεύον χαρακτηριστικό p, στοιχεία $a, b \in R$ και $n \in \mathbb{N}$, ισχύει:
$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \;\&\; (a - b)^n = a^{p^n} - b^{p^n}$$

Ξεκινώντας για $q = p^n$ θεωρώντας $x^q - x$ στο $F_p[x]$ και το F να είναι το διαχωριζόμενο πεδίο του F_p. Η πολυωνυμική θα έχει q ξεχωριστές ρίζες στο πεδίο F από την στιγμή που η παράγωγος $(x^q - x) = qx^{q-1} - 1 = -1$ στο $F_p[x]$ και βάσει της υπόδειξης 1 δεν μπορεί να έχει κοινή ρίζα με το πολυώνυμο $x^q - x$. Έστω τώρα σύνολο $S = \{a \in F : a^q - a = 0\}$. Το σύνολο αυτό είναι προφανώς υπο-πεδίο του F, λόγω:

- $0,1 \in S$
- Για $a, b \in S$ ισχύει $(a - b)^q = a^q - b^q = a - b \ \in S$
- Για $a, b \in S$ $με$ $b \neq 0$, ισχύει $(ab^{-1})^q = a^q b^{-q} = ab^{-1} \in S$

Όμως το πολυώνυμο $x^q - x$ πρέπει να διαχωρίζεται στο S, λόγω του ότι το σύνολο περιέχει τις ρίζες του πολυωνύμου. Αναγκαστικά έχω $S = F$ και επειδή το S έχει q στοιχεία, τότε και το F είναι πεπερασμένο πεδίο με q στοιχεία.

(Απόδειξη Μοναδικότητας): Υπενθυμίζονται τα εξής:

1. Ένα πεπερασμένο πεδίο F έχει, για χαρακτηριστικό p με p πρώτο αριθμό, σύνολο στοιχείων p^n όπου n η τάξη του πεδίου.
2. Για πεδίο K και f πολυώνυμο θετικού βαθμού στο $K[x]$, τότε υπάρχει διαχωριζόμενο πεδίο πάνω από το K. Γενικά οποιαδήποτε δύο διαχωριζόμενα πεδία πάνω από το K είναι ισομορφικά βάσει ισομορφισμού που κρατά τα στοιχεία του K σταθερά και "χαρτογραφεί" τις ρίζες στο καθένα

Οπότε έχω:

Για F ένα πεπερασμένο πεδίο με $q = p^n$ στοιχεία. Το F έχει χαρακτηριστικό p και από την υπόδειξη 1, έχω θπο-πεδίο F_p. Από το προηγούμενο λήμμα το πεδίο έχει διαχωριζόμενο πεδίο του πολυωνύμου $x^q - x$ πάνω στο F_p. Πλέον από την υπόδειξη 2 έχω μοναδικότητα του διαχωριζομένου πεδίου.

Θεώρημα(Κριτήριο Υπο-πεδίου): Για F_q ένα πεπερασμένο πεδίο με $q = p^n$ στοιχεία, έχω ότι οποιοδήποτε υπο-πεδίο του F_q έχει τάξη p^m, όπου m είναι θετικός διαιρέτης του n. Αντιστρόφως, για m θετικό διαιρέτη του n, υπάρχει ένα ακριβώς υπο-πεδίο του F_q με συνολικά p^m στοιχεία.

(Απόδειξη): Υπενθυμίζεται από πριν το εξής:

- Για F ένα πεπερασμένο πεδίο που περιλαμβάνει το υποπεδίο K με q στοιχεία. Τότε το F έχει q^m στοιχεία, όπου $m = [F: K]$

(Ευθύ): Το υποπεδίο K ενός πεπερασμένου πεδίου F είναι τάξης p^m για θετικό ακέραιο $m \leq n$. Από την υπόδειξη γνωρίζω $q = p^m$ πρέπει να είναι δύναμη του p^m και έτσι το m είναι αναγκαστικά διαιρέτης του n.

(Αντίστροφο): Εάν m είναι ένας θετικός διαιρέτης του n, τότε $p^m - 1$ διαιρεί το $p^n - 1$ και τότε για τα πολυώνυμα έχω $x^{p^m-1} - 1$ να διαιρεί το $x^{p^n-1} - 1$ στο $F_p[x]$. Συνεπώς κάθε ρίζα του πολυωνύμου $x^{p^m} - x$ είναι και ρίζα του $x^q - x$ το οποίο ανήκει στο F_p. Αυτό συνεπάγεται ότι το πεδίο F_p περιέχει ένα υπο-πεδίο ένα διαχωριζόμενο πεδίο του $x^{p^m} - x$ στο πεδίο F_p. Βάσει του θεωρήματος ύπαρξης και μοναδικότητας ένα τέτοιο διαχωριζόμενο υπο-πεδίο θα έχει τάξη p^m. Στη περίπτωση που έχω δύο διαφορετικά υποπεδία στο πεδίο F_p τάξεως p^m, τα οποία μαζί περιέχουν περισσότερες από p^m ρίζες του πολυωνύμου $x^{p^m} - x$ στο πεδίο F_p κάτι το οποίο μας οδηγεί σε άτοπο.

Παρατήρηση: Με την παραπάνω απόδειξη κατανοεί κανείς ότι το μοναδικό υποπεδίο του αρχικού F_{p^m} με τάξη p^m, όπου το m είναι διαιρέτης του n, συνίσταται ακριβώς από τις ρίζες του πολυωνύμου $x^{p^m} - x \in F_p[x]$ στο F_{p^n}.

<u>Θεώρημα</u>: Για κάθε πεπερασμένο πεδίο F_q η πολλαπλασιαστική ομάδα F_q^* των μη μηδενικών στοιχείων του πεδίου F_q θα είναι κυκλική.

(Υπόδειξη): Αναφέραμε ότι μια πολλαπλασιαστική ομάδα (με πράξη τον πολλαπλασιασμό) είναι κυκλική εάν:

$$\forall\, b \in G, \exists\, j \in \mathbb{N}\ με\ b = a^j, \text{ όπου } a \text{ είναι το στοιχείο γεννήτρια της κυκλικής ομάδας}$$

(Απόδειξη): Υποθέτουμε ότι μιλάμε για αρχικό πεδίο με αριθμό στοιχείων $q \geq 3$. Έστω λοιπόν η ποσότητα $h = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_m^{r_m}$ είναι ο πρωταρχικός παράγοντας της τάξεως $h = q - 1$ της ομάδας F_q^*.

- Τότε $\forall i, 1 \leq i \leq m$, το πολυώνυμο $x^{\frac{h}{p_1}} - 1$ θα έχει το πολύ $\frac{h}{p_1}$ ρίζες στο πεδίο F_q. Προφανώς $\frac{h}{p_i} < h$, πράγμα που σημαίνει ότι υπάρχουν μη-μηδενικά στοιχεία στο στο πεδίο F_p που να μην είναι ρίζες του παραπάνω πολυωνύμου. Έστω λοιπόν a_i ένα τέτοιο στοιχείο για το οποίο θέτουμε $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Τότε, έχω $b_i^{p_i^{r_i}} = 1$, από την στιγμή που η τάξη του b_i είναι διαιρέτης του $p_i^{r_i}$ και είναι προφανώς της μορφής $p_i^{s_i}, 0 \leq s_i \leq r_i$. Από την άλλη $b_i^{p_i^{r_i-1}} = a^{\frac{h}{p_i}} \neq 1$, πράγμα που σημαίνει ότι η τάξη του b_i είναι $p_i^{r_i}$. Θεωρούμε ότι το στοιχείο $b = b_1 \cdot b_2 \cdot \ldots \cdot b_m$ είναι τάξης h και τότε είναι ένας διαιρέτης τουλάχιστον ενός από τους m ακεραίους της μορφής $\frac{h}{p_i}, 1 \leq i \leq m$ έστω του $\frac{h}{p_1}$. Τότε έχω:

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} \cdot \ldots \cdot b_m^{\frac{h}{p_1}}$$

- Στη περίπτωση που $2 \leq i \leq m$, τότε $p_i^{r_i}$ διαιρεί την ποσότητα $\frac{h}{p_1}$, με $b_i^{p_i^{r_i}} = 1$. Οπότε $b^{\frac{h}{p_1}} = 1$ και η τάξη του b_1 πρέπει να διαιρεί την $\frac{h}{p_1}$, πράγμα αδύνατο επειδή η τάξη του b_1 είναι $p_1^{r_1}$. Αναγκαστικά η ομάδα F_q^* είναι μια κυκλική ομάδα με γεννήτρια b.

ΚΕΦΑΛΑΙΟ 4 Ελλειπτικές καμπύλες σε πεδία Galois

4.1 Η εικόνα των ελλειπτικών καμπυλών πάνω σε πεδία Galois

Από τη στιγμή που μελετήθηκαν οι ελλειπτικές καμπύλες και τα πεπερασμένα πεδία Galois, πρέπει να μελετηθεί και το μαθηματικό υπόβαθρο που στηρίζει την απεικόνιση των καμπυλών σε αυτά τα πεδία την στιγμή που αποτελούν τα απαραίτητα μαθηματικά εργαλεία που οδηγούν στην επίλυση του διακριτού λογαριθμικού προβλήματος ελλειπτικών καμπυλών (ECDSA).

4.2 Εξίσωση Weirstrass

(Ορισμός των ρητών σημείων – rational points): Ένα F-ρητό σημείο είναι ένα σημείο (x, y) μιας αλγεβρικής καμπύλης $f(x, y) = 0$, όπου οι συντεταγμένες του σημείου βρίσκονται σε πεπερασμένο πεδίο F και επιπλέον ικανοποιούν την εξίσωση της καμπύλης όντας συγχρόνως ρητοί αριθμοί.

(Εξίσωση Weierstrass): Για ένα αυθαίρετο (πεπερασμένο) πεδίο F ορίζουμε την εξίσωση Weierstrass της ελλειπτικής καμπύλης E επί του επιπέδου, δηλαδή E/F, που είναι της μορφής:

$$E: y^2 + a_1 \cdot xy + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6 \; με \; (x, y)$$

Όπου:

$$Για \; \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6 \in F \; να \; ισχύει \; \Delta \neq 0, με \; \Delta \; να \; είναι \; η \; διακρίνουσα \; της \; E.$$

Η τιμή της διακρίνουσας αυτής, είναι:

$$\Delta = -d_2^2 \cdot d_8 - 8 \cdot d_4^3 - 27 \cdot d_6^2 + 9 \cdot d_2 \cdot d_4 \cdot d_6$$

$$με \begin{cases} d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1 \cdot a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2 \cdot a_6 + 4a_2 \cdot a_6 - a_1 \cdot a_3 \cdot a_4 + a_3^2 \cdot a_2 - a_4^2 \end{cases}$$

Σε περίπτωση που για το πεδίο F έχω επέκταση, έστω L τότε το σύνολο των L −ρητών σημείων δίνεται από την εξίσωση:

$$E(L) = \{(x, y) \in L \times L : \; y^2 + a_1 \cdot xy + a_3 \cdot y - x^3 - a_2 \cdot x^2 - a_4 \cdot x + a_6 = 0\} \cup \{\infty\}$$

Όπου ∞ είναι το σημείο-άπειρο(γεωμετρικός τόπος).

Παρατήρηση: Η προϋπόθεση ότι η διακρίνουσα $\Delta \neq 0$ στηρίζει το γεγονός ότι η ελλειπτική καμπύλη είναι λεία, ότι δηλαδή δεν υπάρχουν σημεία στα οποία η ίδια να παρουσιάζει δύο ή περισσότερες διακριτές εφαπτόμενες ευθείες.

4.2.1 Ισομορφισμοί Weirstrass

Συχνά για τους σκοπούς της εκάστοτε έρευνας, δεδομένου της πολυπλοκότητας της εξίσωσης Weirstrass είναι απαραίτητος ο μετασχηματισμός της σε πιο "φιλικές" στο χρήστη μορφές, οι οποίες δομούνται βάση του παρακάτω ισομορφισμού.

(Ισομορφισμός Weierstrass – Αλλαγή Μεταβλητών): Για δύο διακριτές μεταξύ τους ελλειπτικές καμπύλες μορφής Weierstrass, έστω E_1, E_2, πάνω σε πεπερασμένο πεδίο F με τύπους:

$$E_1: y^2 + a_1 \cdot xy + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6$$
$$E_2: y^2 + a_1{}' \cdot xy + a_3{}' \cdot y = x^3 + a_2{}' \cdot x^2 + a_4{}' \cdot x + a_6{}'$$

Οι καμπύλες καλούνται ισομορφικές πάνω στο πεδίο εάν υπάρχουν τιμές $u, r, s, t \in F, με\ u \neq 0$, ώστε για το μετασχηματισμό:

$$(x, y) \rightarrow (u^2 \cdot x + r, u^3 \cdot y + u^2 \cdot s \cdot x + t)$$

Ξεκινώντας από την E_1 καταλήγουμε στην E_2. Σε γενικές γραμμές εάν μια εξίσωση ικανοποιεί τις προϋποθέσεις και τον τύπο των παρακάτω εξισώσεων τότε αποτελεί ελλειπτική καμπύλη. Επιπλέον βασικός παράγοντας στην επιλογή των ισομορφισμών αποτελεί το χαρακτηριστικό του πεδίου, έστω K.

Περίπτωση 1 – Χαρακτηριστικό $\mathbf{K} \in \{2, 3\}$: στην προκυμμένη περίπτωση γνωρίζοντας ότι η διακρίνουσα $\Delta = -16(4a^3 + 27b^2)$, χρησιμοποιούμε τον ισομορφισμό:

$$(x, y) \rightarrow \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1 \cdot x}{216} - \frac{a_1^3 + 4a_1 \cdot a_2 - 12a_3}{24}\right)$$

Ο παραπάνω μετασχηματισμός οδηγεί στην γνωστή μορφή των ελλειπτικών καμπυλών:

$y^2 = x^3 + a \cdot x + b.$

(Εφαρμογή): Θεωρώ την ελλειπτική καμπύλη E πάνω στο πρωτεύων πεδίο F_{29}. Τότε για τιμές $p = 29, a = 4\ και\ b = 20$, θεωρώ την ελλειπτική καμπύλη:

$$E: y^2 = x^3 + 4x + 20\ στο\ F_{29}$$

Υπολογίζω ότι $\Delta = -16(4a^3 + 27b^2) = -176896 \neq 0\ (mod\ 29)$. Άρα η καμπύλη είναι ελλειπτική.

Περίπτωση 2 – Χαρακτηριστικό $K = 3$: Στη συγκεκριμένη περίπτωση ανάλογα με την σχέση που συνδέει τις ποσότητες $a_1^2\ και - a_2$, παρατηρώ τις εξής μορφές:

- Για $a_1^2 \neq -a_2$ με την αλλαγή μεταβλητών $(x, y) \rightarrow \left(x + \frac{d_4}{d_2}, y + a_1 \cdot x + a_1 \cdot \frac{d_4}{d_2} + a_3\right)$, με $d_2 = a_1^2 + a_2\ και\ d_4 = a_4 - a_1 \cdot a_3$ προκύπτει:

$$y^2 = x^3 + a \cdot x^2 + b$$

Με $a, b \in F$ και τότε έχω διακρίνουσα $\Delta = -a^3 \cdot b$.

- Για $a_1^2 = -a_2$ με την αλλαγή μεταβλητών $(x, y) \to (x, y + a_1 \cdot x + a_3)$,όπου τότε προκύπτει:

$$y^2 = x^3 + a \cdot x + b$$

Με $a, b \in F$ και τότε έχω διακρίνουσα $\Delta = -a^3$.

Περίπτωση 3 – Χαρακτηριστικό $K = 2$: Στη συγκεκριμένη περίπτωση ανάλογα με την τιμή του συντελεστή a_1, παρατηρώ τις εξής μορφές:

- Για $a_1 \neq 0$ χρησιμοποιώ τον ισομορφισμό $(x, y) \to \left(a_1^2 \cdot x + \frac{a_3}{a_1}, a_1^3 \cdot y + \frac{a_1^2 \cdot a_4 + a_3^2}{a_1^3}\right)$ που οδηγεί στη μορφή:

$$y^2 + x \cdot y = x^3 + a \cdot x^2 + b, \text{όπου } a, b \in F \text{ με } \Delta = b.$$

<u>Παρατήρηση</u>: παραδοχή της παραπάνω μορφής θα αποτελέσει την καμπύλη-κλειδί πάνω στην οποία θα στηριχθεί η εφαρμογή του τελευταίου κεφαλαίου. Στη βιβλιογραφία είναι γνωστλοτερη ως μη-υπερμοναδική (non supersingular).

- Για $a_1 = 0$ χρησιμοποιώ τον ισομορφισμό $(x, y) \to (x + a_2, y)$ που οδηγεί στη μορφή:

$$y^2 + c \cdot y = x^3 + a \cdot x + b, \text{όπου } a, b, c \in F \text{ με } \Delta = c^4.$$

Η παραπάνω μορφή ονομάζεται υπερμοναδική (supersingular).

4.3 Υπόθεση Riemann και θεώρημα Hasse

(Ο χάρτης του Frobenius): ονομάζουμε την εξίσωση τη μορφής:

$$\varphi_p : E(\bar{F}_p) \to E(\bar{F}_p), \text{όπου } \varphi_p(x, y) = (x^p, y^p)$$

Δηλαδή τον ομομορφισμός που δρα πάνω στο πεδίο F_q.

(Η απόλυτη ομάδα Galois επιπέδου F_q): Για F_qένα πεπερασμένο πεδίο $\mathbb{Z}/q\mathbb{Z}$ το οποίο έχει σύνολο στοιχείων q^n για ένα συγκεκριμένο πρώτο αριθμό q, θεωρούμε $\bar{F}_q$ να είναι ένα ορισμένο αλγεβρικό κλείσιμο του παραπάνω πεδίου και για ένα οποιοδήποτε ακέραιο αριθμό n έχω:

$$F_{q^n} = \{x \in \bar{F}_q : x^{q^n} = x\}$$

Η ομάδα Galois συμβολίζεται με $Gal(F_{q^n}/F_q)$ είναι κυκλική τάξεως n, που δημιουργείται από τον αυτομορφισμό $x \to x^q$.

(Ενδομορφισμός Frobenius): Είναι ο ενδομορφισμός $\pi_{q,E} : E \to E$ για τον οποίο γνωρίζω ότι για χαρακτηριστικό πρώτο αριθμό p σε

$F(r) \cong \pi_{q,E}(r) = r^p$, όπου ισχύουν οι ιδιότητες:

- $F(r \cdot s) = (r \cdot s)^p = r^p \cdot s^p = F(r) \cdot F(s)$
- $F(r + s) = (r + s)^p = r^p + s^p = F(r) + F(s)$,

Όπου $r, s \in R$ και E είναι μια ελλειπτική καμπύλη για την οποία ισχύει ο ενδομορφισμός.

Επιστρέφοντας λοιπόν, θεωρούμε E/F_q μια ελλειπτική καμπύλη που διαγράφεται πάνω σε ένα πεπερασμένο πεδίο. Ψάχνουμε τα ρητά σημεία της $E(F_q)$, ισοδύναμα ένα περισσότερο από τον αριθμό των λύσεων της εξίσωσης:

$$E: y^2 + a_1 \cdot xy + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6 \, με \, (x, y) \in F_q^2$$

Εμπειρικά, δεδομένου ότι για μια τυχαία τιμή του x μπορούν να προκύψουν το πολύ δύο τιμές του y, ένα αναμενόμενο άνω φράγμα είναι το:

$$\#E(F_q) \leq 2 \cdot q + 1.$$

Παρατήρηση: Σε γενικές γραμμές, έχει παρατηρηθεί ότι για μια τυχαία τετραγωνική εξίσωση έχει περίπου 50% πιθανότητα να είναι επιλύσιμη στο πεδίο F_q, πράγμα που μας προϊδεάζει ότι το όριο έχει τάξη είναι τελικά μεγέθους q και όχι $2q$, $\approx\rightarrow \ \#E(F_q) \sim q + 1$.

Η υπόθεση του Riemann για ελλειπτικές καμπύλες είναι αυτή που χρησιμοποιείται για να επιλύσει το παραπάνω πρόβλημα, η οποία σε ειδικότερη μορφή της γνωστότερη ως θεώρημα του Hasse μας αποδεικνύει το φράγμα.

Θεώρημα(Υπόθεση του Riemann για ελλειπτικές καμπύλες): Για E μια ελλειπτική καμπύλη που έχει σημεία πάνω σε πεπερασμένο πεδίο F_q, με $\#E(F_{q^n})$ τον αριθμό των σημείων αυτών, ισχύει:

$$\left|\#E(F_{q^n}) - 1 - q^n\right| \leq 2 \cdot q^{\frac{n}{2}}, \forall n \geq 1.$$

(Απόδειξη): Για μια δοσμένη ενδεχομένως ελλειπτική καμπύλη δοσμένη υπό μορφή εξίσωσης Weierstrass με συντεταγμένες στο πεδίο F_q. Γνωρίζοντας ότι $Gal(\bar{F}_p/F_q)$ τοπολογικά παράγεται από τον ενδομορφισμό $\pi_q: x \xrightarrow{\pi_q} x^q$, ένα σημείο $P \in E(\bar{F}_p)$ βρίσκεται στην ελλειπτική $E(F_q)$ εάν $\pi_{q,E}(P) = P$. Οπότε $P \in E(F_{q^n}) \Leftrightarrow \pi_{q,E}^n(P) = P$ άρα $E(F_{q^n}) = Ker(1 - \pi_{q,E}^n)$, από την θεωρεία των kernels(θεωρία που δεν μας απασχολήσει). Γνωρίζουμε σε αυτό το σημείο ότι ισχύει $\#E(F_{q^n}) = \deg(1 - \pi_{q,E}^n)$.

(Υπόδειξη): Για δύο ελλειπτικές καμπύλες E_1, E_2 που διαγράφονται σε ελλειπτικό πεδίο, η συνάρτηση:

$$d: Hom(E_1, E_2) \times Hom(E_1, E_2) \rightarrow \mathbb{Z} \text{ με } (c, d) \mapsto \deg(c + d) - \deg(c) - \deg(d).$$

Έπειτα από την ανησότητα του Cauchy-Schwartz έχω:

$$|\deg(1-\pi_{q,E}^{n})-\deg(1)-\deg(\pi_{q,E}^{n})|\leq 2\cdot\sqrt{\deg(1)\cdot\deg(\pi_{q,E}^{n})}$$

Το οποίο μας οδηγεί στο ζητούμενο. Με επιλογή του $n=1$ θα έχω:

$$\left|\#E(F_q)-1-q\right|\leq 2\cdot\sqrt{q},\forall n\geq 1.-\textbf{Θεώρημα του Hasse}$$

(Ορισμός υπερμοναδικότητας και μη): Για p το χαρακτηριστικό ενός πεδίου F_q και E μια ελλειπτική καμπύλη πάνω σε αυτό ονομάζουμε την καμπύλη $E(F_q)$ υπερμοναδική εάν p διαιρεί t, όπου $|t|\leq 2\cdot\sqrt{p}$ το ίχνος της. Σε αντίθετη περίπτωση η εν λόγω καμπύλη είναι μη-υπερμοναδική.

4.4 Καμπύλες Koblitz

Οι καμπύλες Koblitz είναι μια υποομάδα ελλειπτικών καμπυλών με κυριότερο χαρακτηριστικό την διακριτή κατασκευή τους κάτι το οποίο οδηγεί σε αποτελεσματικές υπολογιστικές διαδικασίες. Βασική διαφορά των Koblitz με εκείνες που χρησιμοποιούνται πολύ πιο συχνά στην κρυπτογραφία είναι ότι οι δεύτερες λαμβάνουν τιμές για τις δομικές τους παραμέτρους από συγκεκριμένους αλγορίθμους. Η χειμαρρώδης ανάπτυξη του κρυπτονομίσματος του Bitcoin στήριξε τις πρακτικές διαδικασίες που αφορούν την ανταλλαγή και την ιδιοκτησία στις καμπύλες του Koblitz και συγκεκριμένα στην ***secp256k1.***

Μαθηματική Ανάλυση

(Ορισμός): Η ονομασία Koblitz, χρησιμοποιείτε για να περιγράψει:

- Δυαδικές ανώμαλες καμπύλες πάνω σε πεδία F_q $με$ $q=2^k$ $και$ $k\geq 160$, υπό την μορφή:
$$y^2+x\cdot y=x^3+a\cdot x+1, με\ a\in\{0,1\}$$
- Ελλειπτικές καμπύλες πάνω σε πεπερασμένα πρωτεύοντα πεδία F_p, υπό την μορφή:
$$y^2=x^3+a\cdot x+b$$

Παρατήρηση: Σχετικά με την πρώτη περίπτωση επιθυμούμε ο k να είναι πρώτος αριθμός για λόγους ασφαλείας. Στην περίπτωση όμως που είναι σύνθετος παρατηρούμε καλύτερη απόδοση. Γενικά επιλέγουμε παραμέτρους προκυμμένου να έχουμε αποδοτικά υπολογιστικό ενδομορφισμό μέχρι η τάξη της καμπύλης να είναι πρώτος αριθμός. Συνήθως εργαζόμαστε με τον πρώτο τύπο των καμπυλών.

(Θεωρητικό Παράρτημα): Σε αυτό το σημείο παρατίθενται οι ορισμοί του Χάρτη και του Ίχνους του Frobenious.

Ορισμός: Χάρτη του Frobenious ονομάζουμε την συνάρτηση:

$$\tau_p: E\left(\overline{F_p}\right), \text{όπου } \tau_p(x,y) = (x^p, y^p)$$

Που αποτελεί ομομορφισμό ομάδας. Η ποσότητα $a_p = p + 1 - \#E(F_q)$ ονομάζεται ίχνος Frobenious. Ο υπολογισμός της προκύπτει από την χρήση ενός χάρτη Frobenious για την παραγωγή γραμμικού μετασχηματισμού σε συγκεκριμένο διανυσματικό χώρο $V_l(E)$. Το a_p είναι το ίχνος του παραπάνω γραμμικού μετασχηματισμού.

Επιπλέον από τα θεωρήματα των Hasse kai Birch, ισχύουν:

$$\left|a_p\right| \leq 2 \cdot \sqrt{p} \text{ και } \#\{E/F_q : a \leq a_p(E) \leq b\} \approx \frac{1}{\pi}\int_a^b \sqrt{4p - t^2}\, dt \text{ με } a, b \in \mathbb{R}$$

Παρατήρηση: Υπολογίζεται ότι υπάρχουν συνολικά $2p$ διαφορετικές καμπύλες πάνω στο πεδίο F_p, ενώ η ποσότητα $a_p(E)$ παίρνει τιμές που ακολουθούν την παραπάνω κατανομή.

Συνεχίζοντας η εύρεση της τάξης των καμπυλών Koblitz έχει υπολογιστεί ως:

$$\#E(F_{2^k}) \equiv ord\left(E\left(GF(2^k)\right)\right) = 2^k - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k, \mu\varepsilon\ i = \sqrt{i^2} = \sqrt{-1},$$

Η υπολογιστική υπεροχή τους όταν ορίζονται σε πεδία F_{2^k} είναι η ύπαρξη του ομομορφισμού:

$$\tau: E\left(F_q\right) \to E\left(F_q\right), \mu\varepsilon\ \tau(x,y) = (x^2, y^2) \in E$$

Όπου τ είναι ο χάρτης του Frobenious. Οπότε σε τελικό στάδιο για σημείο $P = (x,y) \in E$, έχω:

$$P(x,y) \to Q(x^2, y^2) \mu\varepsilon\ P, Q \in E(F_q)$$

Τώρα όσον αφορά τον σημειακό πολλαπλασιασμό (point multiplication) των καμπυλών Koblitz, η συνάρτηση-χάρτης τ είναι ιδιαίτερα χρήσιμη. Συγκεκριμένα για $\tau(x,y) = (x^2, y^2)$ που ικανοποιεί την σχέση $\tau^2 + 2 = \mu \cdot \tau$ και λύση $\tau = \frac{\mu \pm \sqrt{-7}}{2}$ και $P(x,y)$ σημείο της καμπύλης, έχω:

$$\tau\left(\tau(P)\right) \oplus [2] \cdot P = [\mu] \cdot \tau \cdot P \Leftrightarrow [\tau^2 + 2] \cdot P = [\mu\tau] \cdot P$$

Παράδειγμα: Για $19 = \tau^4 + 1$ ισούται με $[19] \cdot P = \left(x^{2^4}, y^{2^4}\right) + (x,y)$.

Φυσικά δεν παύει να ισχύει η συνεπαγωγή, όπου για $l \in \mathbb{Z}$, μορφής $l = l_0 + l_1 \cdot \tau + \cdots + l_r \cdot \tau^r$ με $l_0, l_1, \ldots, l_r \in \{0, \pm 1\}$, όπου $l \cdot P = l_0 \cdot P + l_1 \cdot \tau(P) + \cdots + l_r \cdot \tau_r(P)$.

Επιλογή των δομικών παραμέτρων

Η γενική ιδέα, όπως προαναφέρθηκε, είναι η συνεχής δοκιμή παραμέτρων μέχρι να προκύψει ένας υπολογίσιμος ενδομορφισμός προκυμμένου να έχω καμπύλη με τάξη πρώτο αριθμό. Οι

παράμετροι αυτοί για καμπύλη πάνω σε πεδίο F_p έχουν $[\log_2 p] \in [192,224,256,384,521]$. Πειραματικά έχει παρατηρηθεί ότι για $[log2] = 2 \cdot t$ συνεπάγεται t ψηφία ασφάλειας, δηλαδή κατά την επίλυση του διακριτού λογαριθμικού προβλήματος ελλειπτικών καμπυλών με t ψηφία θα χρειαστούν 2^t πράξεις-δοκιμές.

Ορισμός (Συμπαράγοντας): Για καμπύλη Koblitz, έστω E_a, που έχει τάξη πρώτο αριθμό πάνω σε πεδίο F_{2^m}, εάν έχω σύνολο σημείων $\#E_a(F_{2^m}) = h \cdot n$ με n πρώτο αριθμό και $h = \begin{cases} 4, \text{ όταν } a = 0 \\ 2, \text{όταν } a = 1 \end{cases}$, η ποσότητα h ονομάζεται συμπαράγοντας.

Συγκεκριμένα για το Bitcoin, οι τιμές όλων των παραμέτρων της secp256k1: $y^2 = x^3 + a \cdot x + b$ είναι:

- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- $a = 0$
- $b = 7$
- $h = 1$
- $G = 10632455806$
- $n = 4294967295$

ΚΕΦΑΛΑΙΟ 5 ECDSA

5.1 Αλγόριθμος ελλειπτικών καμπυλών ECDSA

Τα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών, γνωστότερα ως (ECC), δίνουν με τη χρήση ελλειπτικών καμπυλών τα ανάλογα αποτελέσματα σε σχέση με τα αντίστοιχα προγενέστερα αλγορίθμων διακριτών λογαρίθμων (DLC). Αυτό πραγματοποιείται με αντικατάσταση της υποομάδας Z_p^* με το σύνολο των σημείων μιας ελλειπτικής καμπύλης πάνω σε πεπερασμένο πεδίο Galois. Η θεωρητική βάση της ασφάλεια αυτών των αλγορίθμων είναι η ανθεκτικότητα του αντίστοιχου διακριτού προβλήματος που αναλύεται παρακάτω.

Το διακριτό λογαριθμικό πρόβλημα ελλειπτικών καμπυλών

(Διατύπωση): Θεωρώ μια ελλειπτική καμπύλη E ορισμένη πάνω σε ένα πεπερασμένο πεδίο F_p, χαρακτηριστικού p δηλαδή:

$$E: y^2 = x^3 + A \cdot x + B, όπου\ A, B \in F_p \text{ με περιορισμό } 4 \cdot A^3 + 27 \cdot B^2 \neq 0$$

Για δύο σημεία της $E(F_p)$, έστω P, Q αναζητώ τον ακέραιο $x, x \in \mathbb{N}$ για τον οποίο:

$$Q = x \cdot P$$

Παρατήρηση: Υπενθυμίζεται ότι ο μικρότερος ακέραιος x που επαληθεύει το παραπάνω πρόβλημα ονομάζεται διακριτός λογάριθμος του σημείου Q σε σχέση με το σημείο P. Συμβολίζεται με:

$$m = \log_S(T) = ind_S(T).$$

Δομικά στοιχεία μιας $E(F_p)$, ιδιαίτερα κατά την εφαρμογή του αλγορίθμου, είναι οι τομεακές παράμετροι (domain parameters), συγκεκριμένα:

1. Το μέγεθος του πεδίου $q, q = 2^m$ ή $q = p$
2. Οι τιμές των συντελεστών A, B με τιμές στο πεπερασμένο πεδίο F_q. Ισχύει όμως η διακριτοποίηση:
$$\begin{cases} y^2 = x^3 + A \cdot x + B, για\ p > 3 \\ y^2 + x \cdot y = x^3 + A \cdot x + B, για\ p = 2 \end{cases}$$
3. Το γενεσιουργό σημείο $G = G(x_g, y_g)$ με τάξη πρώτο αριθμό, με συντεταγμένες στο πεδίο $E(F_q)$.
4. Η τάξη n του σημείου G, όπου $n > 2^{160}\ και\ n > 4 \cdot \sqrt{q}$
5. Ο συντελεστής $h = \#E(F_q)/n$

Για την επίλυση του διακριτού λογαριθμικού προβλήματος ελλειπτικών καμπυλών έχουν επινοηθεί τρεις μέθοδοι και υλοποιηθεί οι αντίστοιχοι λογάριθμοι.

Θεωρητικό Υπόβαθρο (Συμβολισμός Landau): Σε επίπεδο λογαρίθμων χρησιμοποιείται για να περιγράψει τον αναμενόμενο χρόνο και χρόνο αλγορίθμων. Γενικότερα ισχύουν τα εξής:

Για δύο συναρτήσεις $f(x), g(x)$ με $x \in \mathbb{R}\text{^} *$ ένα υποδιάστημα του συνόλου των πραγματικών αριθμών, ισχύει:

Για x→∞

$$|f(X)| \leq C \cdot |g(x)| \ \forall x > N, \text{όπου } C, N \text{ πραγματικοί αριθμοί}$$

Πράγμα που σημαίνει ότι η f δεν μεγαλώνει γρηγορότερα από την αντίστοιχη g. Αντίστοιχα για $x \to a, a \in R$ υπάρχουν σταθερές $d > 0$ και C, ώστε:

$$|f(x)| \leq C \cdot |g(x)| \ \forall x, \text{ώστε } |x - a| < d$$

Στη συγκεκριμένη εργασία θα μας απασχολήσουν μόνο δύο είδη του συμβολισμού:

$$O(n\text{^}c): \text{πολυωνιμική και } O(n): \text{γραμμική}$$

Παρατήρηση: Συνήθως εκφράζει την τάξη (order) μιας συνάρτησης, δηλαδή τον ρυθμό αύξησης της. Εναλλακτικά υπολογίζουμε το πιθανό σφάλμα των προσεγγίσεων για τις τιμές που προκύπτουν από μια εξίσωση.

5.2 Ανάλυση των Μεθόδων - Επιθέσεων

(Εξαντλητική Μέθοδος): Υπολογίζοντας τα γινόμενα $x_1 \cdot P, x_2 \cdot P, x_3 \cdot P, \ldots$ για τυχαίες τιμές $x_1, x_2, x_3, \ldots$ μέχρι να επαληθευτεί για κάποια τιμή η ισότητα $x \cdot P = Q$. Η χρονική διάρκεια μέχρι την παραπάνω επαλήθευση είναι $O(p)$, από την στιγμή που έχει αποδειχθεί ότι $\#E(q) = O(p)$. Ξεκάθαρα η πιο χρονικά απαιτητική μέθοδος που προϋποθέτει ισχυρό υπολογιστικό σύστημα για συγκρίσιμα αποτελέσματα σε σχέση με τις επόμενες.

(Μέθοδος Μικρού & Μεγάλου Βήματος): Αρχικά μετασχηματίζουμε την ισότητα $Q = x \cdot P$ που θέλουμε να επαληθεύσουμε, ως εξής:

$$Q = x \cdot P \ \Leftrightarrow$$

$$Q = (a \cdot m + b) \cdot P \ \Leftrightarrow$$

$$Q - a \cdot m \cdot P = b \cdot P$$

Υπενθύμιση: Γενικά οποιοσδήποτε ακέραιος $x, x \in \mathbb{Z}$ μπορεί να γραφεί ως γινόμενο τριών αυθαίρετων ακεραίων $a, m, b\ \mathbb{Z}$, έτσι ώστε $x = a \cdot m + b$.

Οπότε σε επόμενο στάδιο δημιουργούμε δύο διανυσματικές λίστες των αρχικών σημείων P, Q της $E(F_q)$ με τους προηγούμενους συντελεστές $(x_1, x_2, x_3, \ldots)$, δηλαδή:

$$\boldsymbol{\Delta\iota\acute{\alpha}\nu\upsilon\sigma\mu\alpha\ 1}: x_1 \cdot P, x_2 \cdot P, x_3 \cdot P, \ldots$$
$$\boldsymbol{\Delta\iota\acute{\alpha}\nu\upsilon\sigma\mu\alpha\ 2}: Q - x_1 \cdot P, Q - x_2 \cdot P, Q - x_2 \cdot P, \ldots$$

Περιμένουμε μέχρι να βρεθεί σύγκρουση της μορφής:

$$x_i \cdot P = Q - x_j \cdot P, \text{όπου } i, j = 1,2,3, \dots$$

Παρατήρηση: Ανάλογα με την τιμή του α, έχω:

- Για $a = 0$ έχω $Q = b \cdot P, με\ b = [0, m]$, ουσιαστικά συγκρίνω το Q με τα σημεία του διαστήματος $0 \cdot P, \dots, m \cdot P$
- Για $a = 1$ έχω $Q = m \cdot P + b \cdot P, με\ b = [0, m]$, ουσιαστικά συγκρίνω το Q με τα σημεία του διαστήματος $m \cdot P, \dots, 2 \cdot m \cdot P$
- Συνεχίζοντας για $a = m - 1$ έχω $Q = (m-1) \cdot m \cdot P + b \cdot P, με\ b = [0, m]$, ουσιαστικά συγκρίνω το Q με τα σημεία του διαστήματος $(m-1) \cdot m \cdot P, \dots, m^2 \cdot P$

Παρατήρηση: Ουσιαστικά ελέγχω όλα τα σημεία από το $0 \cdot P, \dots, n \cdot P$ εκτελώντας $2 \cdot m$ προσθέσεις και πολλαπλασιασμούς. Ο αναμενόμενος χρόνος εκτέλεσης είναι $O(\sqrt{q})$ και είναι σαφώς μικρότερος από τον αντίστοιχο της εξαντλητικής μεθόδου.

(Μέθοδος του Pollard – Pollard's P Method): αποδεδειγμένα χρειάζεται για ίδιο χρόνο εκτέλεσης $O(\sqrt{q})$ και χώρο αποθήκευσης κατά την εκτέλεση $O(\sqrt{q})$. Γενικότερα η μέθοδος του Pollard όταν εφαρμόζεται σε διακριτούς λογαρίθμους εκτελείται σε κοινό χρόνο με τους υπόλοιπες μεθόδους, αλλά δεσμεύει λιγότερο χώρο συγκριτικά με αυτές, που είναι $O(1)$.

(Θεωρητικό Υπόβαθρο και Ανάλυση): Αρχικά θα πρέπει να γνωρίζει κανείς την έννοια του πρωτεύοντα παράγοντα ενός θετικού ακεραίου. Συγκεκριμένα:

$$Για\ n \in \mathbb{Z}^+, θετικός\ ακέραιος\ ισχύει:$$

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}, \text{όπου } p_i: πρώτοι\ αριθμοί\ και\ a_i: οι\ τάξεις\ των\ p_i$$
$$(Factorization\ Algorithm)$$

Οι αριθμοί p_i ονομάζονται πρωτεύοντες παράγοντες του θετικού ακεραίου n. Γενικά με αυτή την μέθοδο αναζητούμε τους p_i.

Πιο συγκεκριμένα ένας τέτοιος παράγοντας p για τον αρχικό ακέραιο n, μπορεί να βρεθεί εάν ο $p-1$ είναι το αποτέλεσμα που προκύπτει από μικρούς πρώτους αριθμούς βρίσκοντας έναν m, όπου:

- $p - 1 | q, με\ q \gg 1, q \in \mathbb{R}\ και\ (c, n) = 1.$
- $p - 1 | q, m = 1 (mod\ p), οπότε\ p | m - 1$

Και υπάρχει μεγάλη πιθανότητα $n \neq m - 1$ και στην προκυμμένη περίπτωση $ΜΚΔ(m-1, n)$ θα είναι μη τετριμμένος διαιρέτης του ακεραίου n.

Τώρα σε επίπεδο αλγορίθμου με τη μέθοδο ψάχνω διακριτά ζεύγη $(a, A)\ και\ (b, B)$ ακεραίων $modulo\ n$ για να επαληθεύσω την ισότητα:

$$a \cdot P + b \cdot Q = A \cdot P + B \cdot Q, με\ a, b, A, B \in \mathbb{Z}$$

Διώχνω την ποσότητα $Q = x \cdot P$ και στην συνέχεια και την P, δηλαδή:

$$a \cdot P + b \cdot x \cdot P = A \cdot P + B \cdot x \cdot P \Leftrightarrow$$

$$(a + b \cdot x) \cdot P = (B - b) \cdot x \cdot P \Leftrightarrow$$

$$(a - A) = (B - b) \cdot x\ (mod\ n) \Leftrightarrow$$

$$x = (a - A) \cdot (B - b)^{-1} mod\ n$$

Ως εκ τούτου $x = \log_P Q$ υπολογίζεται όπως παραπάνω.

("Βίαιη" Επίθεση): Για την εύρεση των παραπάνω ζευγών μπορούμε για τυχαίους ακεραίους $c, d \in [0, n-1]$ να αποθηκεύσουμε τις τριάδες $(c, d, c \cdot P + d \cdot Q)$ σε ένα πίνακα. Η διαδικασία σταματά όταν ένα από τα αποθηκευμένα ζεύγη επαναληφθεί, δηλαδή καταλήξουμε σε σύγκρουση (collition). Σύμφωνα με το "Παράδοξο των Γενεθλίων" - Birthday Paradox ο αναμενόμενος χρόνος μέχρι την σύγκρουση είναι $\approx \sqrt{\pi \cdot n/2}$ και ο αποθηκευτικός χώρος τριπλασιάζεται για τον χρόνο αυτό.

(Pollard's Attack): Η επίθεση του Pollard παρόλο που θα βρει σύγκρουση στον ίδιο χρόνο χρειάζεται αμελητέο αποθηκευτικό χώρο. Η γενική ιδέα της μεθόδου είναι για δοσμένο σημείο $X \in < P >$ και ακεραίους (c, d) με $X = c \cdot P + d \cdot Q$ να οριστεί **τυχαία** επαναληπτική συνάρτηση $f: < P > \rightarrow < P >$ η οποία εύκολα να υπολογίζει $X = f(X)$ και $\bar{c}, \bar{d} \in [0, n-1]$ με $\bar{X} = \bar{c} \cdot P + \bar{d} \cdot Q$.

Στη συνέχεια ορίζουμε τυχαία διαμέριση του $< P >$, έστω $\{S_1, S_2, \dots, S_L\}$ προκυμμένου τα L σύνολα να έχουν έστω και προσεγγιστικά το ίδιο μέγεθος. Συνήθεις τιμές του L είναι $16(2^4)$ και $32(2^5)$.

<u>Παράδειγμα</u>: Για $L = 32$ και σημείο $X \in < P >$ μπορεί να ανατεθεί σε σύνολο S_j της παραπάνω διαμέρισης εάν τα κάποια από τα ψηφία της τετμημένης του σημείου παριστάνουν τον ακέραιο $j - 1$. Μπορούμε για συνάρτηση διαμέρισης G, να γράψουμε $G(X) = j$ *εάν* $X \in S_j$. Επιπλέον για $1 \leq j \leq L$ έστω $a_j, b_j \in_{\mathbb{R}} [0, n-1]$. Τότε η επαναληπτική συνάρτηση f, ορίζεται ως:

$$f(X) = X + a_j \cdot P + b_j \cdot Q\ όπου\ j = G(X)$$

<u>Παρατήρηση</u>: Εάν $X = c \cdot P + d \cdot Q$ έχω $f(X) = \bar{X} = \bar{c} \cdot P + \bar{d} \cdot Q$ όπου $\bar{c} = c + a_j\ mod\ n$ και $\bar{d} = d + b_j\ mod\ n$.

Τελικά κάθε σημείο $X_0 \in < P >$ καθορίζει μια ακολουθία $\{X_i\}_{i \geq 0}$ σημείων, όπου $X_i = f(X_{i-1})$ για $i \geq 1$. Επειδή το σύνολο $< P >$ είναι πεπερασμένο θα καταλήξουμε σίγουρα σε σύγκρουση. Μετά μπαίνουμε σε ένα κύκλο πράξεων που θα καταλήγουν στην ίδια σύγκρουση πάλι.

Παρατήρηση: Αυτό σημαίνει ότι θα υπάρχει ένας μικρός δείκτης w για τον οποίο $X_w = X_{w+s}$ για ένα $s \geq 1$. Καταλήγοντας έχουμε:

$$X_i = X_{i-s} \; \forall i \geq w + s.$$

Το w ονομάζεται "μήκος της ουράς", ενώ το s είναι το "μήκος του κύκλου". Γενικά σύγκρουση αναμένουμε μετά από $\sqrt{\pi \cdot n/2}$ όρους, ενώ τα μήκη ουράς και κύκλου είναι αντίστοιχα $t \sim \sqrt{\pi \cdot n/8}$ και $s \sim \sqrt{\pi \cdot n/8}$. Ο αλγόριθμος που χρησιμοποιείται για την εύρεση της εν λόγο σύγκρουσης είναι ο "Αλγόριθμος εύρεσης κύκλου του Floyd".

Μεθοδολογία: Συνοπτικά υπολογίζουμε ζεύγη σημείων (X_i, X_{2i}) για $i = 1,2,3, \ldots$ και σταματάμε όταν $X_i = X_{2i}$. Σύγκρουση έχουμε όταν για δύο σημεία $X_i, X_j \rightarrow X_i = X_j \; για \; i \neq j$. Η μέθοδος στο σημείο που πλεονεκτεί χωρικά είναι ότι διαγράφει όλα τα προηγούμενα ζεύγη σημείων για τα οποία δεν προέκυψε σύγκρουση. Ο αναμενόμενος αριθμός των ζευγών που θα συγκρίνουμε είναι $k \in [w, w + s]$ και για τυχαία επαναληπτική f είναι $1.0308 \cdot \sqrt{n}$. Ως εκ τούτου ο αναμενόμενος αριθμός των ομαδικών λειτουργιών ελλειπτικής καμπύλης είναι περίπου $3 \cdot \sqrt{n}$.

Μια πιο φιλική στον αναγνώστη διατύπωση του είναι ο αλγόριθμος "Χελώνας & Λαγού".

(Αλγόριθμος Χελώνας-Λαγού): Προκυμμένου να αποφύγουμε την χρονοβόρα δοκιμή όλων των πιθανών τιμών a, b ως εισόδους της εξίσωσης ζεύγους δεδομένου ότι έχω n^2 υποψήφια ζεύγη πράγμα που θα είχε χρονική πολυπλοκότητα $O(n^2)$ μεγαλύτερη από την αντίστοιχη της εξαντλητικής μεθόδου, προχωράμε ως εξής:

- Αρχικά για την αρχική ακολουθία των ζευγών (a, b) υπολογίζω την πρώτη παράσταση $a \cdot P + b \cdot Q$.
- Υλοποιούμε την "χελώνα" μια συνάρτηση του αλγορίθμου για τον παραπάνω υπολογισμό, που διαβάζει ένα-ένα τα ζεύγη (a, b) και υπολογίζει τις αντίστοιχες τιμές της παράστασης.
- Υλοποιούμε και τον "λαγό", ένα αντίστοιχο αλγόριθμο του προγράμματος, με την διαφορά ότι είναι ταχύτερος διότι προσπερνά κάθε επόμενο ζεύγος του αρχικού (a, b) υπολογίζοντας το δεύτερο κατά σειρά κάνοντας έτσι λιγότερους υπολογισμούς σε σχέση με την χελώνα.

Αναμενόμενα θα καταλήξουμε σε δύο ζεύγη $(a, b) - (A, B)$ για τα οποία θα επαληθεύεται η αρχική ισότητα. Είναι απτό να καταλήξει κανείς στο συμπέρασμα ότι ο χρόνος της διαδικασίας είναι $O(\sqrt{n})$ και ο χώρος που απαιτείται για την αποθήκευση των ζευγών $O(\log n)$.

5.3 Πλεονεκτήματα και μειονεκτήματα του ECDSA

Στη προσπάθεια για ασφαλή παραγωγή και διαχείριση της πληροφορίας και στην περίπτωση μας της επικοινωνίας των συμβαλλομένων, η σύγχρονη κρυπτογραφία παρέχει μέσα από τις δομές της ένα εύρωστο σύνολο τεχνικών για την αντιμετώπιση οποιασδήποτε κακόβουλης ενέργειας κατά των χρηστών. Φυσικά αυτό δεν σημαίνει ότι δεν υπάρχουν και μειονεκτήματα του αλγορίθμου, τα οποία κατά γενική ομολογία είναι πολύ λιγότερα από τα πλεονεκτήματα.

Πλεονεκτήματα του ECDSA:

1. Σε σχέση με προγενέστερα κρυπτογραφικά εργαλεία όπως το RSA, DSA, οι αλγόριθμοι ελλειπτικών καμπυλών προσφέρουν μεγαλύτερη ασφάλεια για συγκεκριμένο μέγεθος κλειδιών. Κάτι τέτοιο παρατηρείται και για μικρά μεγέθη κλειδιών τα οποία εξ ορισμού είναι πολύ πιο ευάλωτα σε σχέση με τα μεγαλύτερου μεγέθους.
2. Ο χρόνος και ο χώρος στη μνήμη που απαιτούνται για την παραγωγή και διακίνηση των μηνυμάτων στην περίπτωση του ECDSA είναι σαφώς λιγότερος σε σχέση με παλαιότερα εργαλεία.
3. Είναι σαφές επίσης ότι απαιτείται λιγότερη υπολογιστική ισχύ, μνήμη άρα και εξειδικευμένα συστήματα προκυμμένου να υλοποιηθούν οι απαραίτητες διαδικασίες κάνοντας έτσι την πλατφόρμα προσιτή σε περισσότερους χρήστες και ερευνητές.
4. Από οικονομικής πλευράς τα συστήματα που στηρίζονται σε αλγορίθμους ελλειπτικών καμπυλών είναι οικονομικότερα σε σχέση με τους παλαιότερους αλγορίθμους στους τομείς του αποθηκευτικού χώρου και των εξόδων ψύξης και ενέργειας.

Μειονεκτήματα του ECDSA:

1. Τα κρυπτογραφικά εργαλεία είναι κατά κύριο λόγο ελεύθερα στην πρόσβαση από κάθε είδους χρήστες, αφήνοντας ανοιχτό το περιθώριο δημιουργίας εργαλείων με σκοπό την παραβίαση κάθε είδους πλατφόρμας.
2. Μια κρυπτογραφημένη πληροφορία, αυθεντική και ψηφιακά υπογεγραμμένη μπορεί να είναι δύσκολη στην πρόσβαση ακόμη και για έναν νόμιμο χρήστη σε κρίσιμη στιγμή λήψης αποφάσεων, ιδιαίτερα όταν η πλατφόρμα έχει παραβιαστεί.
3. Η κρυπτογραφία εξ' ορισμού δεν προστατεύει από τα τρωτά σημεία και τις απειλές που προκύπτουν από την κακή σχεδίαση συστημάτων, πρωτοκόλλων και διαδικασιών.

5.4 Επιλογή κατάλληλων τομεακών παραμέτρων

Κρυπτογραφικές εφαρμογές και αλγόριθμοι που στηρίζουν την ασφάλεια παραγωγής, διαχείρισης και αποστολής προσωπικών κλειδιών και μηνυμάτων στο διακριτό λογαριθμικό πρόβλημα ελλειπτικών καμπυλών ECDLP, συχνά έρχονται αντιμέτωπές με μεθοδικές επιθέσεις όπως η επίθεση Pollard's Rho οι οποίες επιλύουν το παραπάνω πρόβλημα και "σπάνε" τον αλγόριθμο κάνοντας τον ευάλωτο.

Για την ζητούμενη ασφάλεια επιθυμούμε να μην είναι εύκολη η επίλυση του και για το λόγο αυτό δομούμε αναλόγως τις εκάστοτε ελλειπτικές καμπύλες πάνω στο πρωτεύοντα πεδία Galois προκυμμένου να ικανοποιούν συγκεκριμένους περιορισμούς.

(Γενική Ιδέα): Επιθυμώ ο αριθμός των σημείων $\#E(F_p)$ της ελλειπτικής καμπύλης επί του πεδίου να διαιρείται από μεγάλο αριθμό $n, n > 2^{160}$. Ονομάζουμε επιπλέον "μέγιστη αντίσταση" του αλγορίθμου την παρακάτω συνθήκη:

- Για ελλειπτική καμπύλη E πάνω σε πρωτεύων πεδίο F_p για την οποία ισχύει: $\#E(F_q) = h \cdot n$, όπου $\begin{cases} n\ \pi\rho\acute{\omega}\tau o\varsigma \\ h \in \{1,2,3,4\} \end{cases}$

Τέλος, χρησιμοποιώ τιμές συντελεστών για την καμπύλης εξόδους μιας one way συνάρτησης κατακερματισμού, όπως η SHA-1 ώστε να έχω πλήρη τυχαιότητα.

Συνθήκες Ασφαλείας

Επιθυμώ να ισχύουν:

1. Για την τάξη n, να ισχύει $n > 2^L, L \geq 160$
2. Επίσης για την n, θέλω $n > 4 \cdot \sqrt{p}$ ώστε $\#E(F_p) \leq \left(\sqrt{p} + 1\right)^2$) από θεώρημα Hasse γιατί τότε n^2 δεν διαιρεί την ποσότητα $\#E(F_p)$.
3. Για την παραπάνω ποσότητα L, που προέρχεται από ελλειπτική καμπύλη E πάνω σε πρωτεύων πεδίο F_p με τάξη $\#E(F_p)$ που διαιρείται από L-bits πρώτο αριθμό (γενικά ισχύει $\#E(F_p) \approx p$.

(Παρατήρηση): Επιπλέον από την στιγμή που $\#E(F_q) = h \cdot n$, θα βρίσκεται στο διάστημα του Hasse, αυτό σημαίνει ότι υπάρχει μοναδικός υποψήφιος h, ώστε $\#E(F_q) = h \cdot n$, $h = [\frac{(\sqrt{p}+1)^2}{n}]$, όπου σύμφωνα με το θεώρημα οι τάξεις $\#E(F_q)$ κατανέμονται στο διάστημα:

$$\left[p + 1 - 2 \cdot \sqrt{p}, q + 1 + 2 \cdot \sqrt{p}\right]$$

ΚΕΦΑΛΑΙΟ 6 Επιθέσεις επί του ECDSA

6.1 Παραγωγική εφαρμογή αλγορίθμου ECDSA

Όπως προαναφέρθηκε ο αλγόριθμος διακριτού λογαρίθμου ελλειπτικών καμπυλών ECDSA χρησιμοποιείται για όλα τα στάδια παραγωγής και διαχείρισης μηνυμάτων μεταξύ των χρηστών της πλατφόρμας του Bitcoin. Μια αναπαράσταση της διαδικασίας είναι απαραίτητη για καλύτερη κατανόηση των μαθηματικών εργαλείων που στηρίζουν τον αλγόριθμο αλλά φυσικά και πιθανών επιθέσεων που μπορούν να τον παραβιάσουν(hacking) βλάπτοντας την αξιοπιστία του.

Βασικές Λειτουργίες

Για τις ανάγκες της έρευνας χρησιμοποιούμε περιβάλλον γλώσσας Python. Η μορφή της ελλειπτικής καμπύλης που χρησιμοποιούμε είναι:

$$y^2 = x^3 + a \cdot x^2 + b \cdot x + c, με\ a, b, c \in \mathbb{Z}\ πάνω\ σε\ F_p, p\ πρώτος$$

Παρατήρηση: Ο παραπάνω τύπος αφορά μη υπερμοναδικές ελλειπτικές καμπύλες που εφαρμόζονται σε πρωτεύοντα πεδία, γνωστές για τα καλά πειραματικά αποτελέσματα και την ασφάλεια που προσφέρουν στις εφαρμογές του αλγορίθμου.

(Παράδειγμα): Θεωρώ την ελλειπτική καμπύλη $y^2 = x^3 + 4 \cdot x^2 + 3 \cdot x + 10$ πάνω στο πεδίο F_{113}. Τα σημεία σημεία της καμπύλης πάνω στο πεδίο Galois (rational points) μπορούν επίσης να υπολογιστούν.

Σε επίπεδο εντολών:

```
>>> C=CurveOverFp(4,3,10,113)

y^2 = x^3 + 4x^2 + 3x + 10 over F_113

>>> C.show_points()

['Inf', '(1,40)', '(1,73)', '(3,46)', '(3,67)', '(6,7)', '(6,106)', '(8,24)', '(8,89)', '(11,29)', '(11,84)',
'(13,53)', '(13,60)', '(14,23)', '(14,90)', '(15,6)', '(15,107)', '(17,49)', '(17,64)', '(19,11)', '(19,102)',
'(22,2)', '(22,111)', '(23,24)', '(23,89)', '(24,27)', '(24,86)', '(26,49)', '(26,64)', '(29,39)', '(29,74)',
'(30,23)', '(30,90)', '(31,8)', '(31,105)', '(33,20)', '(33,93)', '(34,14)', '(34,99)', '(35,54)', '(35,59)',
'(36,54)', '(36,59)', '(38,54)', '(38,59)', '(40,40)', '(40,73)', '(43,22)', '(43,91)', '(47,6)', '(47,107)',
'(48,42)', '(48,71)', '(52,31)', '(52,82)', '(54,34)', '(54,79)', '(58,43)', '(58,70)', '(59,48)', '(59,65)',
'(62,21)', '(62,92)', '(63,32)', '(63,81)', '(64,33)', '(64,80)', '(65,23)', '(65,90)', '(66,49)', '(66,64)',
'(67,48)', '(67,65)', '(68,40)', '(68,73)', '(69,42)', '(69,71)', '(71,55)', '(71,58)', '(77,50)', '(77,63)',
'(78,24)', '(78,89)', '(79,22)', '(79,91)', '(80,14)', '(80,99)', '(81,31)', '(81,82)', '(86,15)', '(86,98)',
'(88,12)', '(88,101)', '(89,31)', '(89,82)', '(90,25)', '(90,88)', '(93,45)', '(93,68)', '(95,36)', '(95,77)',
'(96,48)', '(96,65)', '(100,22)', '(100,91)', '(104,16)', '(104,97)', '(105,42)', '(105,71)', '(108,14)',
'(108,99)', '(109,26)', '(109,87)']
```

Για κατανόηση των πράξεων της πρόσθεσης και του πολλαπλασιασμού μεταξύ σημείων της καμπύλης και της δημιουργίας υποομάδας που παράγεται από αρχικό σημείο της επί του πεδίου χρησιμοποιούμε τις παρακάτω εντολές:

>>> P=Point(52,82)

>>> C.contains(P)

True

>>> Q=Point(105,71)

>>> C.contains(Q)

True

>>> print C.add(P,Q)

(8,24)

>>> print C.mult(P,3)

(30,90)

>>> C.generate(Q)

['Inf', '(105,71)', '(23,89)', '(64,33)', '(79,22)', '(24,86)', '(109,26)', '(71,55)', '(108,14)', '(31,105)', '(30,90)', '(59,65)', '(86,15)', '(40,73)', '(36,59)', '(68,73)', '(58,70)', '(90,88)', '(77,63)', '(47,107)', '(81,31)', '(89,31)', '(6,7)', '(95,77)', '(54,34)', '(13,60)', '(93,68)', '(17,64)', '(1,40)', '(33,20)', '(100,22)', '(104,97)', '(11,84)', '(88,12)', '(43,91)', '(48,71)', '(69,42)', '(66,64)', '(15,6)', '(38,59)', '(78,89)', '(52,82)', '(8,24)', '(96,65)', '(34,14)', '(22,2)', '(63,81)', '(62,21)', '(14,90)', '(26,64)', '(19,11)', '(29,74)', '(80,99)', '(35,54)', '(67,48)', '(65,90)', '(3,67)', '(3,46)', '(65,23)', '(67,65)', '(35,59)', '(80,14)', '(29,39)', '(19,102)', '(26,49)', '(14,23)', '(62,92)', '(63,32)', '(22,111)', '(34,99)', '(96,48)', '(8,89)', '(52,31)', '(78,24)', '(38,54)', '(15,107)', '(66,49)', '(69,71)', '(48,42)', '(43,22)', '(88,101)', '(11,29)', '(104,16)', '(100,91)', '(33,93)', '(1,73)', '(17,49)', '(93,45)', '(13,53)', '(54,79)', '(95,36)', '(6,106)', '(89,82)', '(81,82)', '(47,6)', '(77,50)', '(90,25)', '(58,43)', '(68,40)', '(36,54)', '(40,40)', '(86,98)', '(59,48)', '(30,23)', '(31,8)', '(108,99)', '(71,58)', '(109,87)', '(24,27)', '(79,91)', '(64,80)', '(23,24)', '(105,42)']

Δημιουργία και διαχείριση μηνυμάτων

Τώρα για το Bitcoin ο αλγόριθμος εξυπηρετεί την ανάγκη της υπογραφής των συναλλαγών που πραγματοποιούνται. Παρακάτω χρησιμοποιούμε την secp256k1 καμπύλη που χρησιμοποιείται στο κρυπτονόμισμα αλλά την ορίζουμε σε ένα πολύ μικρότερο πεδίο Galois καθαρά για πειραματικούς λόγους. Σκοπός είναι να παράγουμε ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού που συμβολίζουμε με $(d, Q) = (private\ key, public\ key)$.

Παρατήρηση: Ισχύει $d < order(P) - τάξη\ της\ υποομάδας\ του\ σημείου\ P$ και $Q = d \cdot P$. Θεωρούμε παρά την αλλαγή του πεδίου εφαρμογής ότι η ασφάλεια του αλγορίθμου δεν επηρεάζεται. Σε επίπεδο εντολών:

>>> C=CurveOverFp(0,0,7,1601)

y^2 = x^3 + 7 over F_1601

>>> P=Point(30,307)

>>> C.contains(P)

True

>>> n=C.order(P)

>>> n

801

>>> key=generate_keypair(C,P,n)

Priv key: d = 650

Publ key: Q = (835,1170)

Σε επόμενο στάδιο παράγουμε ένα μήνυμα που επιθυμούμε να στείλουμε και το υπογράφουμε για το παραπάνω ζεύγος κλειδιών. Επίσης σημαντικό να επαληθεύσουμε και την εν λόγο συναλλαγή.

>>> msg='Good morning.Ready for the money transfer.'

>>> sig=sign(msg,C,P,n,key)

ECDSA sig: (Q, r, s) = ((835,1170), 17, 94)

>>> verify('Good morning.Ready for the money transfer.',C,P,n,sig)

True

Παρατηρήσεις:

- Οι ψηφιακές υπογραφές που παράγει ο ECDSA αποτελούνται από το δημόσιο κλειδί Q και από δύο θετικούς ακεραίους (r, s) που παίρνουν τιμές μικρότερες του n, που είναι η τάξη της υποομάδας που παράγεται από το σημείο P. Οι r, s υπολογίζονται από το

ιδιωτικό κλειδί d και το αποτέλεσμα κατακερματισμού (hash) του μηνύματος. Η συνάρτηση κατακερματισμού είναι η SHA-256.

- Επίσης κατά την διαδικασία παραγωγής των ψηφιακών υπογραφών παράγεται η $k, k \in \mathbb{Z}_+$ που ονομάζεται (nonce). Είναι πολύ σημαντικό να παράγεται κάθε φορά που γράφεται και επικυρώνεται μια συναλλαγή με μήνυμα καινούργια τιμή για λόγους ασφάλειας. Οπότε κάθε φορά που χρησιμοποιείται η εντολή **sig** προκύπτουν νέα αποτελέσματα.
- Η εντολή **verify** είναι εξαιρετικά ευαίσθητη σε οποιαδήποτε αλλαγή π.χ. στο περιεχόμενο του μηνύματος γεγονός που συμβάλει στην ασφάλεια της πλατφόρμας.
- Για την δημιουργία μιας νέας πλατφόρμας που θα στηρίξει όλες τις παραπάνω λειτουργίες πάνω σε αλγόριθμο της κρυπτογραφίας ελλειπτικών καμπυλών(ECC) είναι σημαντικό οι προγραμματιστές να διαλέξουν μια από τις ήδη μελετημένες καμπύλες. Ο λόγος δεν είναι άλλος από την τάξη n της υποομάδας του P που χρησιμοποιούν οι αλγόριθμοι. Για να βρει κανείς την τιμή αυτή θα πρέπει να λύσει την εξίσωση $i \cdot P = O, i \in \mathbb{Z}_+ - point\ in\ infinity$. Κάτι τέτοιο προϋποθέτει ασύλληπτη υπολογιστική ισχύ. Αν κάποιος ήταν σε θέση να το πράξει θα μπορούσε πολύ εύκολα να βρει το ιδιωτικό d από το αντίστοιχο δημόσιο Q λύνοντας την εξίσωση. Από μαθηματικής σκοπιάς η δυσκολία του εγχειρήματος εξηγείται από το όριο του Hasse και την θεωρία των πεδίων που αναλύθηκαν σε προηγούμενα κεφάλαια. Θεωρητικά το σύνολο των σημείων του υποσυνόλου του P είναι ίσο με το σύνολο των σημείων όλης της καμπύλης επί του πεδίου, γεγονός που εξηγεί ότι το σύνολο των τιμών των ιδιωτικών κλειδιών d είναι επίσης πολύ μεγάλο.

6.2 Επιθέσεις κατά του αλγορίθμου και πειραματικά διαγράμματα

Παρατηρούμε ότι εάν εξαπολύσουμε μοντελοποιημένη επίθεση επί κατά τεκμήριο ασφαλών κατά NSA καμπυλών, τα αποτελέσματα εξαρτώνται από τις παραμέτρους εφαρμογής. Συγκεκριμένα εάν ελαττώσουμε το μέγεθος των πεδίων Galois και επιλέξουμε τυχαίο σημείο βάσης P(base point) τότε ο ECDSA καθίσταται ευάλωτος. Στην πειραματική μας προσέγγιση επιλέξαμε πεδίο Galois F_{25037} ,καμπύλες των ακόλουθων μορφών και εφαρμόσαμε τις συγκεκριμένες μεθόδους επιθέσεων. Τα αποτελέσματα παρουσιάζονται στον ακόλουθο πίνακα:

Πεδίο Galois F_25037									
						Μέθοδος (Time in sec)			
Όνομα Καμπύλης	Μαθηματικός Τύπος	Σημείο P	Τάξη n	Ιδιωτικό κλειδί d	Δημόσιο κλειδί Q	Brute force	Baby-giant step	Pollard's rho	k
M_221	y^2=x^3+117050x^2+x	(24,813)	1567	79	(10802,5445)	0.946	0.021	0.013	3
M_383	y^2=x^3+2065150x^2+x	(40,19488)	6260	4991	(894,4688)	1.178	0.0232	0.012	4
Curve383187	y^2=x^3+229969x^2+x	(76,37)	12672	11149	(24817,19096)	2.914	0.042	0.018	4
M_511	y^2=x^3+530438x^2+x	(113,3055)	2087	992	(3811,8625)	0.174	0.008	0.009	4
Curve25519	y^2=x^3+486662x^2+x	(141,977)	12488	7728	(25023,18620)	1.975	0.031	0.015	4

Παρατήρηση: Η κρυπτογραφία ελλειπτικών καμπυλών(ECC) στηρίζει την ασφάλεια της στην δυσκολία επίλυσης του διακριτού λογαριθμικού προβλήματος ελλειπτικών καμπυλών(ECDLP). Αυτό σημαίνει ότι η εφαρμογή του ECDSA, αλγόριθμος της ECC που χρησιμοποιείται για την παραγωγή ζεύγους κλειδιών (d, Q), την δημιουργία υπογραφών και την επαλήθευση αυτών των υπογραφών με σκοπό την ασφάλεια των μηνυμάτων των χρηστών θα πρέπει να στηρίζει τις λειτουργίες του σε ένα ανθεκτικό ζεύγος ελλειπτικής καμπύλης και πεδίου Galois σε μοντελοποιημένες επιθέσεις όπως οι παραπάνω.

(Θεωρητικό υπόβαθρο – αλγόριθμος Pohlig-Hellman): Το ECDLP είναι τόσο δύσκολο στην επίλυση του όσο μεγαλύτερη τάξη n, με n πρώτο αριθμό, έχει μία από τις υποομάδες του που όπως αναφέραμε δημιουργείται από την επιλογή του πεδίου βάσης P(base point P).

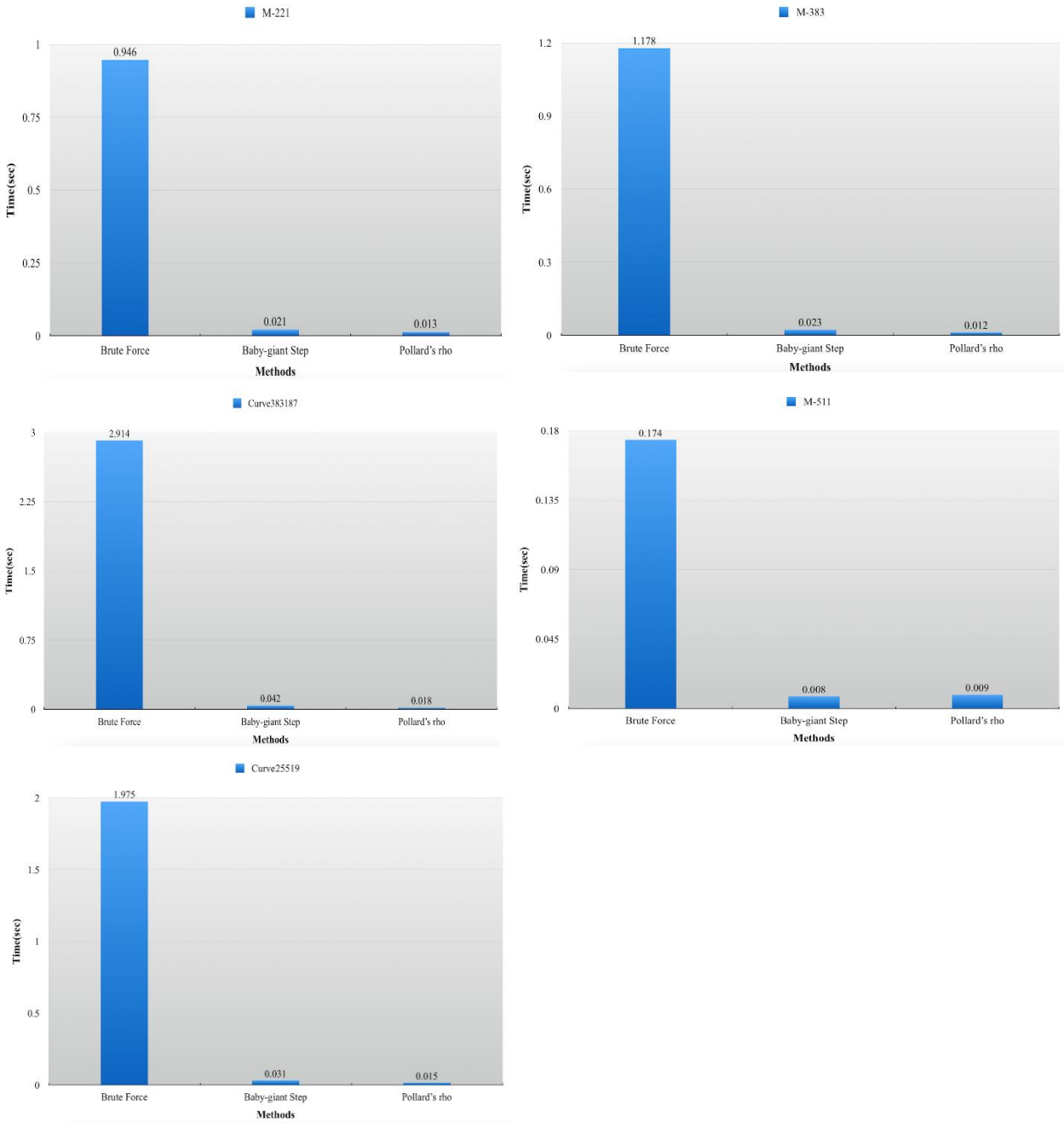
Έστω μια ελλειπτική καμπύλη E πάνω σε πεδίο Galois F_p. Η τάξη της καμπύλης θα είναι ο αριθμός $\#E(F_p) = N$. Η τάξη αυτή μπορεί να παραστεί ως γινόμενο πρώτων αριθμών, δηλαδή $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ που δεν είναι άλλοι από τις τάξεις των υποομάδων που παράγονται από τα σημεία βάσεων(base points P). Όποτε βάσει του παραπάνω αλγορίθμου για να είναι δύσκολο στην επίλυση του το ECDLP, που συνεπάγεται την ανθεκτικότητα του αλγορίθμου ECDSA απέναντι σε μοντελοποιημένες επιθέσεις, θέλουμε οι τάξεις $n_i \equiv p_i$ να είναι "μεγάλοι" πρώτοι αριθμοί.

<u>Παρατήρηση</u>:

- Ισχύει $h = \frac{\#E(F_p)}{n} \Leftrightarrow n \cdot h = \#E(F_p) \in \mathbb{N}$, όπου h είναι το πηλίκο του αριθμού των σημείων της καμπύλης πάνω στο πεδίο, προς την τάξη της υποομάδας του σημείου βάσης. Αυτό συνεπάγεται ότι σε μερικές περιπτώσεις αρκεί να έχω $n = p_1 \cdot p_2 \cdot \ldots \cdot p_n, i \in [1, \ldots, n]$ με κάποιο από τους πρώτους p_i να είναι μεγάλος πρώτος αριθμός. Για ελλειπτικές καμπύλες τύπου Montgomery, με τύπο εξίσωσης $b \cdot y^2 = x^3 + a \cdot x^2 + x, όπου\ b \cdot (a^2 - 4) \neq 0$ πάνω σε πεδίο F_p Galois, έχει αποδειχθεί ότι αρκεί η τάξη της υποομάδας n που παράγει το σημείο P να είναι γινόμενου κάποιου πρώτου αριθμού.

- Όλες οι ελλειπτικές καμπύλες που αναφέρουμε στον παραπάνω πίνακα είναι τύπου Montgomery, κατά συνέπεια δεν είναι απαραίτητο η τάξη n να είναι πρώτος αριθμός.

Διαγραμματική παράθεση του απαιτούμενου χρόνου για την παραβίαση της καμπύλης υπό καθεστώς συγκεκριμένης μοντελοποιημένης επίθεσης.



Συμπερασματικά παρατηρούμε τον πολλαπλάσιο χρόνο που απαιτείται για την παραβίαση του ECDSA υπό καθεστώς μοντελοποιημένης επίθεσης Brute force έναντι των Baby-giant step και Pollard rho, λόγω της φύσης του ελέγχου που εκτελεί, όπως αναλύθηκε στο προηγούμενο κεφάλαιο(Κεφ5 ECDSA). Οι διαφορές των χρόνων των Baby-giant step και Pollard rho είναι πολύ μικρές, όπως ακριβώς προβλέπονται από την σχετική θεωρία.

ΕΠΙΛΟΓΟΣ

Στην εργασία μας ασχοληθήκαμε με το κρυπτονόμισμα Bitcoin την τεχνολογική πλατφόρμα στην οποία φιλοξενείται (Blockchain) και τον αλγόριθμο ECDSA, ο οποίος διασφαλίζει τις συναλλαγές με την παραγωγή ζεύγους ιδιωτικού και δημόσιου κλειδιού. Κύριο χαρακτηριστικό του κρυπτονομίσματος είναι ο αποκεντροτικός χαρακτήρας του και μέσω αυτού η ανθεκτικότητα του σε απόπειρες για έλεγχο και παρέμβαση.

Η κατανεμημένη βάση Blockchain είναι μία βάση δεδομένων σειράς αρχείων και λειτουργεί ως ημερολόγιο όλων των συναλλαγών ή των ψηφιακών γεγονότων που έχουν εκτελεστεί και μοιραστεί μεταξύ των συμμετεχόντων μερών της ομάδας εργασίας. Βασικό χαρακτηριστικό της είναι ότι κάθε είδους συναλλαγή που καταγράφεται επαληθεύεται με την συναίνεση της πλειοψηφίας των συμμετεχόντων στο σύστημα και από την στιγμή εκείνη και μετά δεν διαγράφεται ποτέ.

Οι απόπειρες παραβίασης του κρυπτονομίσματος εστιάζουν σε δύο βασικές θεματικές ενότητες μία αυτής καθ’ αυτής της ψηφιακής πλατφόρμας και δεύτερη κατά του αλγορίθμου διασφάλισης των συναλλαγών.

Χαρακτηριστική επίθεση κατά της πλατφόρμας είναι αυτή της διπλής δαπάνης. Οι επιθέσεις διπλής δαπάνης αποτελούν έναν από τους πιθανούς τρόπους παραβίασης της πλατφόρμας του Bitcoin και γενικότερα του συστήματος των κρυπτονομισμάτων, όπου το ίδιο ποσό που μεταφράζεται σε αντίστοιχο ψηφιακό σήμα δαπανάται δύο ή και περισσότερες φορές κυρίως μέσω της αντιγραφής ή πλαστογράφησης του.

Ο αλγόριθμος ECDSA διασφαλίζει την παραγωγή και διαχείριση της πληροφορίας δια της δημιουργίας ζεύγους ιδιωτικών και δημοσίων κλειδιών τα οποία συνοδεύουν την αποστολή και λήψη των μηνυμάτων που χρησιμοποιούνται στις συναλλαγές. Οι ελλειπτικές καμπύλες επί τον οποίων εδράζεται ο ECDSA αποτελούν το αντικείμενο της επίθεσης των επίδοξων hackers.

Ως μέσω αμύνης επιλέγεται η χρήση ασφαλών ελλειπτικών καμπυλών η οποία περιορίζει αλλά δεν εκμηδενίζει τον κίνδυνο παραβίασης υπό καθεστώς μοντελοποιημένων επιθέσεων.

ΠΗΓΕΣ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΑ

1) A.Narayanan, J.Bonneau, E.Felten, A.Miller, S.Goldfender, “Bitcoin and Cryptocurrency Technologies”, Princeton University,2015
2) R.Lidl, H.Niederreiter, “Introduction to finite fields and their applications”, Press Syndicate of the Cambridge University, 1986. [Online]: http://math.boisestate.edu/~liljanab/MATH508/FiniteFields_and_Applications.pdf
3) D. Hankerson, A.J.Menezes, S.Vanstone, “Guide to elliptic curve cryptography”, Springer-Verlag New York.Inc,2004. [Online]: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3037&rep=rep1&type=pdf
4) J.H.Silverman, “An Introduction to the Theory of Elliptic Curves”, Brown University and NTRU Cryptosystems.Inc,2006.[Online]: https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf
5) C.Grunspan, R.Perez-Marco, “Double spend races”, HAL archives-ouvertes.[Online]: https://hal.archives-ouvertes.fr/hal-01456773
6) “SafeCurves: choosing safe curves for elliptic-curve cryptography”, 2013.[Online]: https://safecurves.cr.yp.to/refs.html
7) A.Khalique, S.Sood, K.Singh, “Implementation of Elliptic Curve Digital Signature Algorithm”, Internatuonal Journal of Computer Applications(0975-8887) Volume 2-No.2,2010. [Online]: http://www.ijcaonline.org/volume2/number2/pxc387876.pdf
8) T.Lim, “A study of Koblitz Curves”,Department of Computer Science, University of California. [Online]: https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Lim.pdf
9) C.Fromknecht, D.Velicanu, S.Yakoubov, “A Decentralized Public Key Infrastructure with Identity Retention”, 2014. [Online]: https://eprint.iacr.org/2014/803.pdf
10) E.Rykwalder, “The Math Behind Bitcoin”, coindesk.com, 2014. [Online]: https://www.coindesk.com/math-behind-bitcoin/
11) “Elliptic Curve”, en.wikipedia.org.[Online]: https://en.wikipedia.org/wiki/Elliptic_curve
12) “Elliptic-curve cryptography”, en.wikipedia.org.[Online]: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
13) “Hasse’s theorem on elliptic curves”, en.wikipedia.org.[Online]: https://en.wikipedia.org/wiki/Hasse%27s_theorem_on_elliptic_curves
14) “Entropy (information theory)”, en.wikipedia.org.[Online]: https://en.wikipedia.org/wiki/Entropy_(information_theory)
15) A.Corbellini, “Elliptic Curve cryptography: a gentle introduction”, Andrea Corbellini's blog, 2015.[Online]: http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/
16) A.Corbellini, “Elliptic Curve Cryptography: breaking security and a comparison with RSA”, Andrea Corbellini's blog, 2015.[Online]: http://andrea.corbellini.name/2015/06/08/elliptic-curve-cryptography-breaking-security-and-a-comparison-with-rsa/
17) “Pollard Rho Factorization Method”, mathworld.wolfram.com, 2018(last updated).[Online]: http://mathworld.wolfram.com/PollardRhoFactorizationMethod.html
18) Qubd, mini_ecdsa/mini_ecdsa.py, github.com, 2017(last updated).[Online]: https://github.com/qubd/mini_ecdsa/blob/master/mini_ecdsa.py