



Σχολή Θετικών Επιστημών

Μεταπτυχιακές Σπουδές στα Μαθηματικά

Διπλωματική Εργασία

***Ελλειπτικές Καμπύλες επί πεπερασμένων σωμάτων και
Κρυπτογραφικές Εφαρμογές***

Αγγελική Αναγνωστάκη

Επιβλέπων καθηγητής: Δημήτριος Πουλάκης

Ηράκλειο, Ιούνιος 2026

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία της φοιτήτριας (Αγγελική Αναγνωστάκη) που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο ΕΑΠ, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.



***Ελλειπτικές Καμπύλες επί πεπερασμένων σωμάτων και
Κρυπτογραφικές Εφαρμογές***

Αγγελική Αναγνωστάκη

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής

*Δημήτριος Πουλάκης
Ομότιμος Καθηγητής
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης*

Συν-Επιβλέπων Καθηγητής

*Ιωάννης Εμμανουήλ
Καθηγητής
Εθνικό και Καποδιστριακό
Πανεπιστήμιο Αθηνών*

Ηράκλειο, Ιούνιος 2026

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Δημήτριο Πουλάκη, για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον και επίκαιρο θέμα, καθώς και για τη συνεχή υποστήριξη, την καθοδήγηση και την πολύτιμη βοήθεια του καθ' όλη τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας.

Περίληψη

Στην παρούσα εργασία παρουσιάζονται οι ελλειπτικές καμπύλες και η χρήση τους στην Κρυπτογραφία. Στο πρώτο κεφάλαιο, δίνεται ο ορισμός των ελλειπτικών καμπυλών, διατυπώνονται οι βασικές ιδιότητες τους, και αναλύονται ορισμένες εναλλακτικές μορφές ελλειπτικών καμπυλών. Το δεύτερο κεφάλαιο αφιερώνεται στην απόδειξη του Θεωρήματος του Hasse. Στο τρίτο κεφάλαιο εξετάζεται το πρόβλημα του Διακριτού Λογαρίθμου στις ελλειπτικές καμπύλες και αναλύονται κάποιες κρυπτογραφικές εφαρμογές, όπως το κρυπτοσύστημα ElGamal, το πρωτόκολλο ανταλλαγής κλειδιών Diffie - Hellman και η ψηφιακή υπογραφή. Τέλος, στο τέταρτο κεφάλαιο διερευνώνται οι ζεύξεις και η χρήση τους στην κρυπτογραφία. Ειδικότερα, μελετάται το ζευγάρι του Weil και η ζεύξη Tate - Lichtenbaum, ενώ αναλύονται βασικά κρυπτογραφικά πρωτόκολλα με τη βοήθεια των pairings.

Λέξεις - Κλειδιά

Ελλειπτικές Καμπύλες, Θεώρημα Hasse, Κρυπτογραφία Ελλειπτικών Καμπυλών, Διακριτός Λογάριθμος, Ψηφιακή Υπογραφή, Κρυπτογραφία βασισμένη σε ζεύξεις

Abstract

This thesis explores elliptic curves and their applications in cryptography. The first chapter introduces the definition of elliptic curves, describes their fundamental properties and examines several alternative forms of elliptic curves. The second chapter focuses on the proof of Hasse's Theorem. The third chapter studies the Elliptic Curve Discrete Logarithm Problem (ECDLP) and analyzes various cryptographic applications, including the ElGamal cryptosystem, the Diffie-Hellman key exchange protocol and digital signatures. Finally, the fourth chapter provides an overview of pairings and their use in cryptography. In particular, the Weil pairing and the Tate-Lichtenbaum pairing are examined and fundamental pairing-based cryptographic protocols are analyzed.

Keywords

Elliptic Curves, Hasse Theorem, Elliptic Curve Cryptography, Discrete Logarithm, Digital Signature, Pairing - Based Cryptography

Περιεχόμενα

Ευχαριστίες	4
Περίληψη	5
Abstract	6
Εισαγωγή	9
1 Ελλειπτικές Καμπύλες	11
1.1 Ελλειπτικές Καμπύλες πάνω από σώματα	11
1.2 Πρόσθεση σημείων πάνω σε Ελλειπτική Καμπύλη	14
1.3 Ισομορφισμοί και j - αναλλοίωτη Ελλειπτικής Καμπύλης	19
1.4 Εξισώσεις Ελλειπτικών Καμπυλών σε Διαφορετικές Μορφές	22
1.4.1 Ελλειπτικές Καμπύλες Edwards	22
1.4.2 Ελλειπτικές Καμπύλες Twisted Edwards	23
1.4.3 Ελλειπτικές Καμπύλες Montgomery	25
1.4.4 Ελλειπτικές Καμπύλες στη μορφή του Legendre	26
1.4.5 Ελλειπτικές Καμπύλες του Hesse	27
2 Ελλειπτικές Καμπύλες επί πεπερασμένων σωμάτων	29
2.1 Ελλειπτικές Καμπύλες ορισμένες πάνω από πεπερασμένα σώματα ...	29
2.2 Θεώρημα Hasse	30
3 Κρυπτογραφικές Εφαρμογές	37
3.1 Πρόβλημα Διακριτού Λογαρίθμου για Ελλειπτικές Καμπύλες	37
3.2 Κωδικοποίηση Κειμένου σε Ελλειπτικές Καμπύλες	37
3.3 Πρωτόκολλο Ανταλλαγής Κλειδιού Diffie-Hellman Ελλειπτικών Καμπυλών	38
3.4 Κρυπτοσύστημα ElGamal Ελλειπτικών Καμπυλών	40
3.5 Κρυπτοσύστημα Menezes Vanstone Ελλειπτικής Καμπύλης	41
3.6 Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης	44
4 Pairing - Based Cryptography	47
4.1 Εισαγωγή στα Pairing	47
4.2 Διγραμμικές Ζεύξεις	47
4.3 Σημεία Στρέψης	49
4.4 Διαιρέτες	50
4.5 Weil Pairing	52
4.6 Tate - Lichtenbaum Pairing	54

4.7 Πρωτόκολλα	55
4.7.1 Τριμερής Ανταλλαγή Κλειδίου	55
4.7.2 Σύντομες Υπογραφές	56
4.7.3 Κρυπτογράφηση με βάση την Ταυτότητα	57
Βιβλιογραφία	60

Εισαγωγή

Η λέξη *κρυπτογραφία* προέρχεται από τα συνθετικά “κρυπτός” + “γράφω” και εστιάζει στη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με κύριο στόχο τη διασφάλιση του απορρήτου των επικοινωνιών. Η κρυπτογραφία εξελίσσεται διαρκώς ως αντικείμενο ερευνητικής εμβάθυνσης. Αυτό οφείλεται στη ραγδαία ανάπτυξη των τηλεπικοινωνιών, όπου η ασφαλής μετάδοση μηνυμάτων διαδραματίζει καθοριστικό ρόλο. Αξίζει να σημειωθεί ότι, η επιστήμη της κρυπτογραφίας καλύπτει ζητήματα αυθεντικότητας, ακεραιότητας και αδυναμίας αποκήρυξης μηνυμάτων.

Οι ελλειπτικές καμπύλες αποτελούν ένα βασικό πεδίο μελέτης στη σύγχρονη μαθηματική έρευνα. Ως αντικείμενο της Θεωρίας Αριθμών και της Αλγεβρικής Γεωμετρίας, συνιστούν ένα χρήσιμο μαθηματικό εργαλείο για την ανάπτυξη της σύγχρονης κρυπτογραφίας. Οι ελλειπτικές καμπύλες επί πεπερασμένων σωμάτων ορισμένες στο $\mathbb{F}_p$ ή στο $\mathbb{F}_{p^n}$ παρουσιάζουν ιδιαίτερο ενδιαφέρον. Σημαντική είναι η ιδιότητα ότι το σύνολο των σημείων τους επί ενός πεπερασμένου σώματος, μαζί με ένα σημείο στο άπειρο, εφοδιασμένο με την πράξη της πρόσθεσης, συγκροτεί μια αβελιανή ομάδα. Η αλγεβρική αυτή δομή είναι το βασικό εργαλείο στο οποίο αναπτύσσονται τα κρυπτογραφικά σχήματα που βασίζονται σε ελλειπτικές καμπύλες. Πέραν της κρυπτογραφίας, οι ελλειπτικές καμπύλες σημειώνουν αυξανόμενο ερευνητικό ενδιαφέρον λόγω της συνεισφοράς τους στην απόδειξη του τελευταίου θεωρήματος του Fermat.

Η κρυπτογραφία ελλειπτικών καμπυλών (ECC) είναι η επιστήμη, η οποία συμβάλλει στην προσπάθεια για παγκόσμια ασφάλεια. Τη δεκαετία του 1980 οι ελλειπτικές καμπύλες εισήχθησαν στην κρυπτογραφία. Πιο συγκεκριμένα, το 1985 αναπτύχθηκε η κρυπτογραφία ελλειπτικών καμπυλών ανεξάρτητα από τους Neal Koblitz και Victor Miller, οι οποίοι πρότειναν τη χρήση των ελλειπτικών καμπυλών για την κατασκευή κρυπτοσυστημάτων δημοσίου κλειδιού, θεμελιώνοντας έτσι ένα νέο ερευνητικό πεδίο.

Η κρυπτογραφία ελλειπτικών καμπυλών βασίζεται στον υπολογισμό λογαρίθμων πάνω σε ένα σύνολο σημείων ελλειπτικής καμπύλης. Η ασφάλεια της βασίζεται στη μη ύπαρξη αλγορίθμου υποεκθετικού χρόνου επίλυσης του προβλήματος του διακριτού λογαρίθμου (ECDLP).

Σημαντικό πλεονέκτημα της κρυπτογραφίας ελλειπτικών καμπυλών είναι ότι χρησιμοποιεί μικρότερες παραμέτρους και κλειδιά επιτυγχάνοντας το ίδιο επίπεδο ασφαλείας σε σχέση με άλλα κρυπτοσυστήματα δημοσίου κλειδιού, όπως το RSA. Αυτό έχει ως αποτέλεσμα να παρατηρείται εξοικονόμηση μνήμης και οι υπολογισμοί να γίνονται γρηγορότερα. Αξιοποιούνται σε κάρτες φορητών υπολογιστών και ασύρματες συσκευές, καθώς η υπολογιστική ισχύ και ο χώρος ολοκληρωμένου κυκλώματος είναι συγκεκριμένος. Χαρακτηριστικά παραδείγματα εφαρμογής της κρυπτογραφίας ελλειπτικών καμπυλών είναι η χρήση έξυπνων καρτών (smart cards) και τα κινητά τηλέφωνα, λόγω των περιορισμένων υπολογιστικών πόρων τους.

Η διαρκής τεχνολογική πρόοδος αναδεικνύει την κρυπτογραφία ελλειπτικών καμπυλών ως έναν ισχυρό και αναπόσπαστο παράγοντα για τη διασφάλιση της μελλοντικής ψηφιακής ασφάλειας.

Κεφάλαιο 1

Ελλειπτικές Καμπύλες

Στο κεφάλαιο αυτό, παρουσιάζεται η βασική θεωρία των ελλειπτικών καμπυλών. Ειδικότερα, εισάγεται ο ορισμός των ελλειπτικών καμπυλών, αναλύεται ο νόμος της πρόσθεσης σημείων πάνω σε μία ελλειπτική καμπύλη και εξετάζονται ορισμένες μορφές ελλειπτικών καμπυλών, όπως η κανονική μορφή Weierstrass.

1.1 Ελλειπτικές καμπύλες πάνω από σώματα

Έστω $\mathbb{F}$ σώμα. Στη συγκεκριμένη ενότητα θεωρούμε ότι το $\mathbb{F}$ είναι ή το $\mathbb{R}$ ή το πεπερασμένο σώμα q στοιχείων $GF(q)$, όπου $q = p^r$ και p πρώτος.

Στο κεφάλαιο 2, αναπτύσσονται πιο αναλυτικά οι ελλειπτικές καμπύλες επί πεπερασμένων σωμάτων.

Ορισμός 1.1 Έστω ένα σώμα $\mathbb{F}$. Μία ελλειπτική καμπύλη $\mathcal{E}$ πάνω στο $\mathbb{F}$ είναι μια ομαλή καμπύλη, η οποία ορίζεται από μια εξίσωση της μορφής:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{F}. \quad (1.1)$$

μαζί με ένα σημείο $\mathcal{O}$ που λέγεται “σημείο στο άπειρο”. Η εξίσωση (1.1) ονομάζεται *μακρά εξίσωση Weierstrass*.

Θα χρησιμοποιήσουμε τους παρακάτω τύπους για να υπολογίσουμε τη διακρίνουσα Δ μιας εξίσωσης της μορφής (1.1):

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Επομένως, η διακρίνουσα Δ δίνεται από τον τύπο:

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

Μία καμπύλη η οποία ορίζεται από μια εξίσωση της μορφής (1.1) είναι ομαλή αν και μόνο αν η διακρίνουσα είναι διάφορη του μηδενός.

Έστω ένα σώμα $\mathbb{F}$ με χαρακτηριστική διάφορη του 2 και του 3 και έστω μία ελλειπτική καμπύλη $\mathcal{E}$ σε Weierstrass μορφή. Τότε αντικαθιστούμε

$$x = u^2 x' + r \quad \text{και} \quad y = u^3 y' + u^2 s x' + t,$$

όπου $u \in \mathbb{F}^*$ και $r, s, t \in \mathbb{F}$. Με αυτή την αλλαγή μεταβλητών εξαλείφονται οι όροι xy, y, x^2 . Επομένως η μακρά εξίσωση Weierstrass απλοποιείται και έτσι καταλήγουμε στον παρακάτω ορισμό.

Ορισμός 1.2 Μια ελλειπτική καμπύλη πάνω από το $\mathbb{F}$ ορίζεται ως το σύνολο των σημείων (x, y) , όπου $x, y \in \mathbb{F}$, τα οποία ικανοποιούν την εξίσωση

$$y^2 = x^3 + Ax + B, \quad \text{όπου } A, B \in \mathbb{F}, \quad (1.2)$$

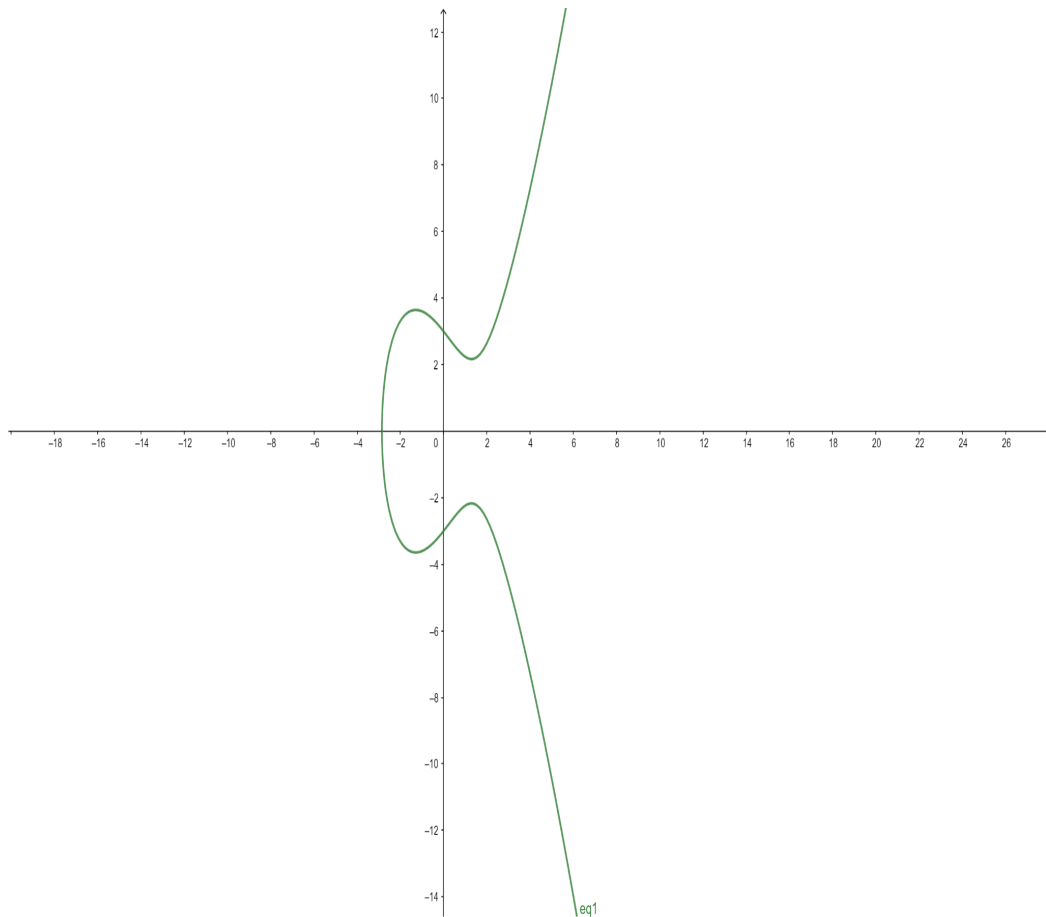
και $4A^3 + 27B^2 \neq 0$, μαζί με ένα στοιχείο $\mathcal{O}$, το οποίο ονομάζεται “σημείο στο άπειρο”.

Η συνθήκη $4A^3 + 27B^2 \neq 0$ εξασφαλίζει ότι η διακρίνουσα

$$\Delta = -16(4A^3 + 27B^2)$$

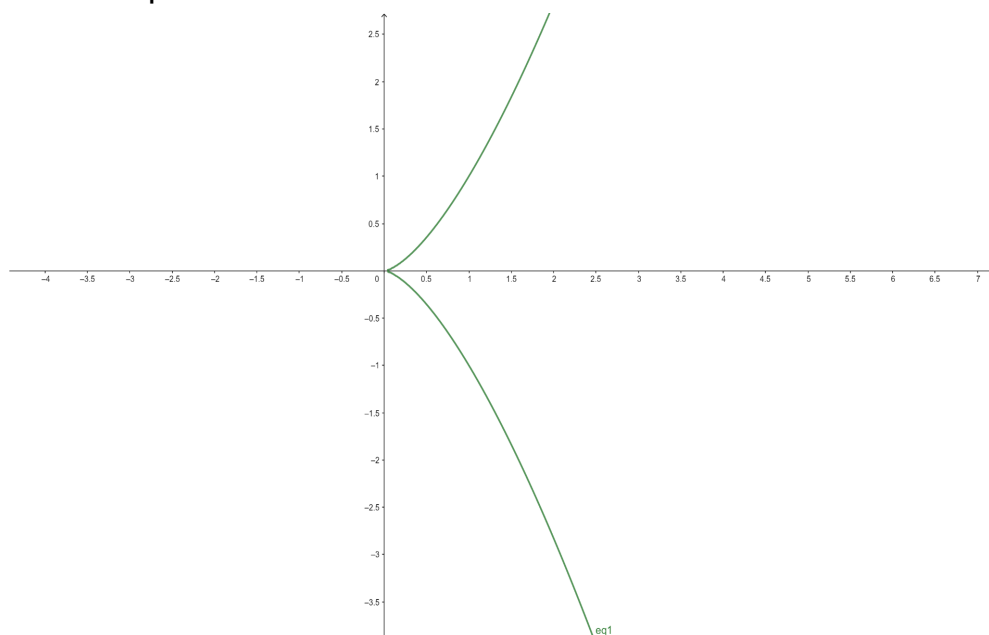
είναι μη μηδενική. Αυτό ισοδυναμεί με την ιδιότητα η αντίστοιχη καμπύλη να είναι χωρίς ανωμαλίες. Η εξίσωση (1.2) ονομάζεται *κανονική μορφή Weierstrass*, με $A, B \in \mathbb{F}$.

Παράδειγμα 1.1 Έστω η ελλειπτική καμπύλη $\mathcal{E}$ πάνω από το $\mathbb{R}$ που ορίζεται από την εξίσωση $y^2 = x^3 - 5x + 9$. Καθώς $\Delta = 1687$, η καμπύλη $\mathcal{E}$ είναι μία ελλειπτική καμπύλη.



Σχήμα 1.1 Μη ιδιάζουσα ελλειπτική καμπύλη, $\Delta \neq 0$

Παράδειγμα 1.2 Η καμπύλη $\mathcal{E} : y^2 = x^3$ έχει διακρίνουσα $\Delta = 0$ και επομένως έχει ανώμαλα σημεία. Ένα τέτοιο σημείο είναι το $(0,0)$. Συνεπώς, η καμπύλη $\mathcal{E}$ δεν είναι ελλειπτική.



Σχήμα 1.2 Ιδιάζουσα καμπύλη, $\Delta = 0$

Στη συνέχεια, διακρίνουμε τις περιπτώσεις:

- Αν το $\mathbb{F}$ είναι σώμα χαρακτηριστικής 2, τότε μια ελλειπτική καμπύλη πάνω από το $\mathbb{F}$ είναι το σύνολο των σημείων, τα οποία ικανοποιούν μια εξίσωση της μορφής

$$y^2 + Cy = x^3 + Ax + B, \quad A, B, C \in \mathbb{F},$$

ή μια εξίσωση της μορφής

$$y^2 + xy = x^3 + Ax + B, \quad A, B \in \mathbb{F},$$

μαζί με ένα “σημείο στο άπειρο” $\mathcal{O}$. Το πολυώνυμο στο δεξί μέλος της εξίσωσης είναι δυνατόν να έχει πολλαπλές ρίζες.

- Αν το $\mathbb{F}$ είναι σώμα χαρακτηριστικής 3, τότε μια ελλειπτική καμπύλη πάνω από το $\mathbb{F}$ είναι το σύνολο των σημείων, τα οποία ικανοποιούν μια εξίσωση της μορφής

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F},$$

μαζί με ένα “σημείο στο άπειρο” $\mathcal{O}$. Το πολυώνυμο στο δεξί μέλος της εξίσωσης δεν έχει πολλαπλές ρίζες.

1.2 Πρόσθεση σημείων πάνω σε ελλειπτική καμπύλη

Έστω δύο σημεία P και Q σε μία ελλειπτική καμπύλη $\mathcal{E}$. Τότε μπορούμε να “προσθέσουμε” και να παράγουμε ένα τρίτο σημείο R στην $\mathcal{E}$. Η έννοια της “πρόσθεσης” εδώ διαφέρει από τη κλασική έννοια της πρόσθεσης. Με τη βοήθεια της γεωμετρίας θα εξηγήσουμε τον ελλειπτικό “προσθετικό νόμο”.

Έστω δύο σημεία

$$P(x_1, y_1) \quad \text{και} \quad Q(x_2, y_2)$$

σε μια ελλειπτική καμπύλη $\mathcal{E}$, η οποία ορίζεται από την εξίσωση

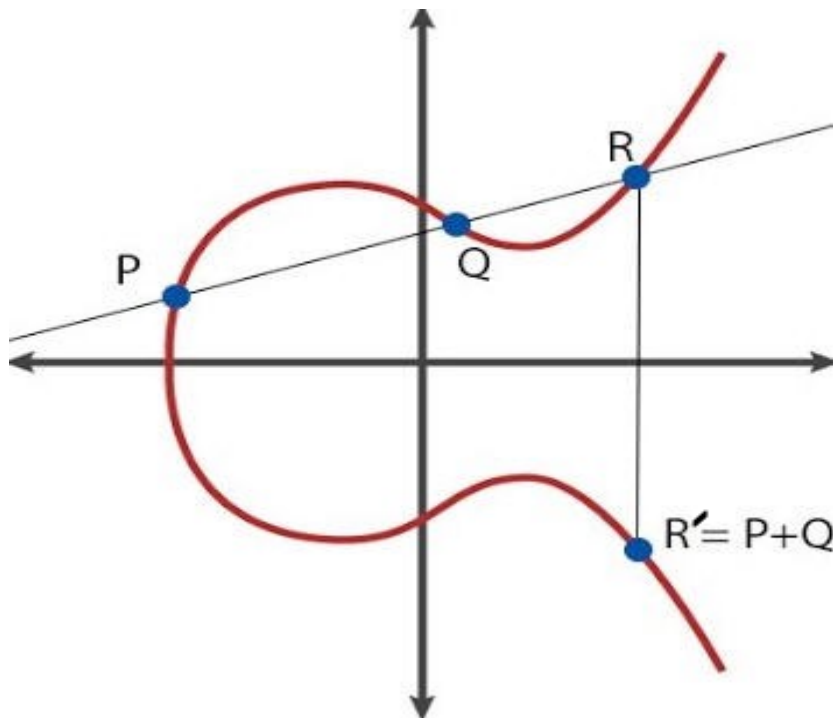
$$y^2 = x^3 + Ax + B.$$

Σχεδιάζουμε την ευθεία L που ενώνει τα σημεία P και Q . Καθώς η εξίσωση της ελλειπτικής καμπύλης E είναι τρίτου βαθμού, η ευθεία L τέμνει την E σε τρία ακριβώς σημεία. Επομένως, η L τέμνει την E σε ένα τρίτο σημείο $R'(x_3, y_3)$. Στη συνέχεια, παίρνουμε το συμμετρικό του σημείου R ως προς τον άξονα $x'x$. Τότε ορίζεται η πρόσθεση σημείων

$$P + Q = R.$$

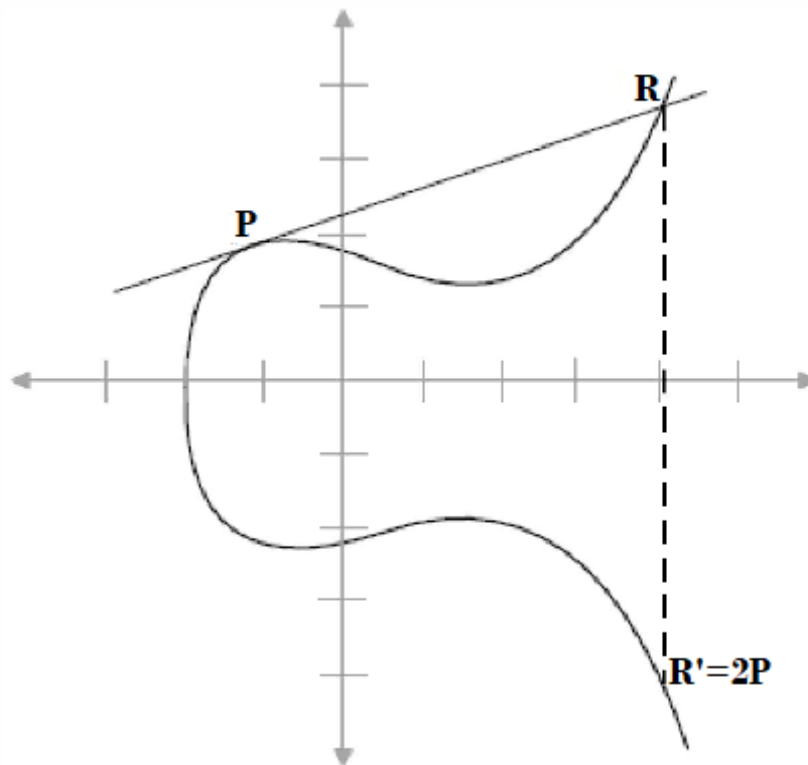
Διακρίνουμε τις περιπτώσεις:

Περίπτωση 1 Έστω δύο διακριτά και μη συμμετρικά ως προς τον άξονα $x'x$ σημεία P, Q πάνω σε μία ελλειπτική καμπύλη E σε κανονική μορφή Weierstrass. Σχεδιάζουμε την ευθεία L που ενώνει τα δύο αυτά σημεία και παρατηρούμε ότι η ευθεία τέμνει την ελλειπτική καμπύλη E σε ένα μοναδικό τρίτο σημείο R . Το συμμετρικό σημείο R' του R ως προς τον άξονα $x'x$ είναι το αποτέλεσμα της πρόσθεσης των σημείων $P + Q$. Δηλαδή, όπως βλέπουμε και στο παρακάτω σχήμα, $R' = P + Q$.



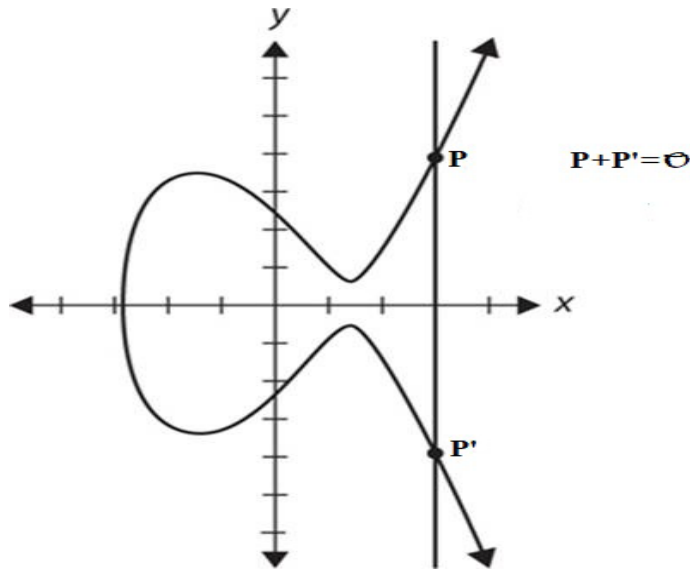
Σχήμα 1.3 Πρόσθεση των σημείων P, Q

Περίπτωση 2 Έστω $P = Q$. Καθώς το σημείο Q τείνει στο P , παρατηρούμε ότι η ευθεία L που διέρχεται από τα P, Q γίνεται εφαπτομένη της ελλειπτικής καμπύλης E στο P . Η ευθεία L τέμνει την ελλειπτική καμπύλη E και πάλι σε τρία σημεία με τη διαφορά ότι το P υπολογίζεται ως διπλό σημείο. Η πράξη $P + P$ ορίζεται κατ' αναλογία με την περίπτωση 1.



Σχήμα 1.4 Πρόσθεση σημείου στον εαυτό του

Περίπτωση 3 Έστω δύο συμμετρικά ως προς τον άξονα $x'x$ σημεία P, P' . Τότε η ευθεία L που διέρχεται από τα P, P' είναι κατακόρυφη και τέμνει την ελλειπτική καμπύλη σε δύο μόνο σημεία. Προκειμένου να αντιμετωπίσουμε το ζήτημα που προκύπτει από αυτό εισάγουμε το σημείο $\mathcal{O}$, το οποίο βρίσκεται στο άπειρο, έτσι ώστε $P + P' = \mathcal{O}$ και θεωρούμε ότι είναι το ουδέτερο στοιχείο της πρόσθεσης.



Σχήμα 1.5 Άθροισμα του σημείου P με το συμμετρικό του P'

Οι παραπάνω κανόνες πρόσθεσης μπορούν να εκφραστούν ως εξής:

Θεώρημα 1.1 (Προσθετικός Αλγόριθμος Ελλειπτικών Καμπυλών)

Έστω μια ελλειπτική καμπύλη E με εξίσωση της μορφής:

$$E: y^2 = x^3 + Ax + B,$$

και έστω $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ δύο σημεία της.

- Αν $P = O$, τότε $P + Q = Q$.
- Αλλιώς θεωρούμε ότι $P, Q \neq O$.
 - Αν $x_1 = x_2$ και $y_1 = -y_2$, τότε θέτουμε $P + Q = O$. Αυτό σημαίνει ότι συμμετρικά σημεία ως προς τον άξονα των x έχουν άθροισμα O .
 - Διαφορετικά,
 - ❖ Αν $P = Q$, τότε θέτουμε $\lambda = (3x_1^2 + A) / (2y_1)$,
 - ❖ Αν $P \neq Q$, τότε θέτουμε $\lambda = (y_2 - y_1) / (x_2 - x_1)$.

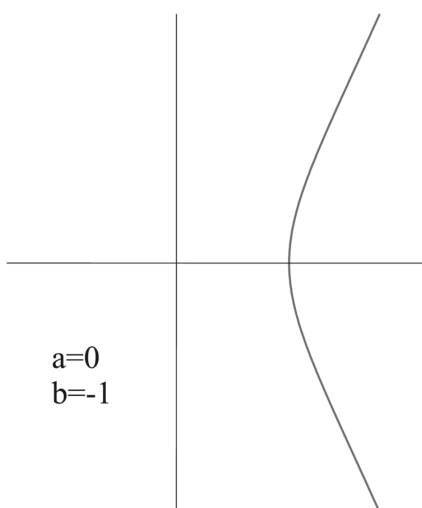
Το σημείο $R = P + Q = (x_3, y_3)$ έχει συντεταγμένες

$$R = (x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1).$$

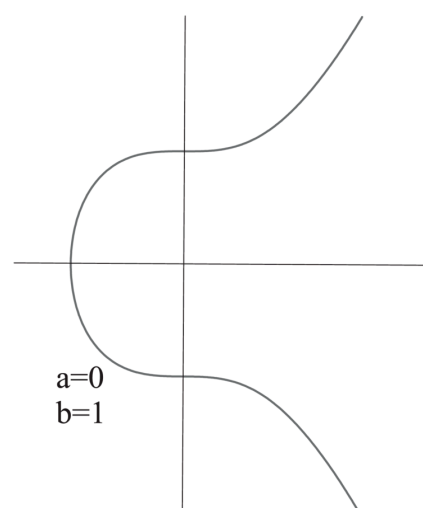
Ορισμός 1.3 Έστω E μία ελλειπτική καμπύλη πάνω από το $\mathbb{R}$, και έστω P, Q δύο σημεία πάνω στην E . Τότε ορίζουμε το $-P$ (το αντίθετο του P) και το άθροισμα $P + Q$ ως εξής:

- 1) Αν $P = \mathcal{O}$, τότε ορίζουμε $-P = \mathcal{O}$ και $P + Q = Q$, δηλαδή το $\mathcal{O}$ είναι το ουδέτερο στοιχείο της ομάδας των σημείων της καμπύλης. Στα παρακάτω θεωρούμε $P \neq \mathcal{O} \neq Q$.
- 2) Το $-P$ είναι το σημείο με την ίδια τετμημένη και αντίθετη τεταγμένη από το P . Από τον ορισμό της ελλειπτικής καμπύλης είναι προφανές πως το $(x, -y)$ ανήκει στην καμπύλη αν και μόνο αν το (x, y) ανήκει στην καμπύλη.
- 3) Αν τα P, Q έχουν διαφορετικές τετμημένες, τότε παρατηρούμε ότι η ευθεία $\ell = \overline{PQ}$ τέμνει την καμπύλη ακριβώς σε ένα ακόμα σημείο R (εκτός αν η ℓ εφάπτεται στο P , συνεπώς έχουμε $R = P$, ή στο Q , άρα έχουμε $R = Q$). Τότε ορίζουμε $P + Q = -R$.
- 4) Αν $Q = -P$, τότε ορίζουμε $P + Q = \mathcal{O}$.
- 5) Αν $P = Q$, η εφαπτομένη στο P θα τέμνει την καμπύλη ακριβώς σε ένα ακόμα σημείο R (εκτός αν το P είναι σημείο καμπής, οπότε παίρνουμε $R = P$). Τότε ορίζουμε $P + Q = -R$.

Παραδείγματα 1.3 Έστω οι ελλειπτικές καμπύλες πάνω από το $\mathbb{R}$ που ορίζονται από τις εξισώσεις $y^2 = x^3 - 1$ (Σχήμα 1.6.1) και $y^2 = x^3 + 1$ (Σχήμα 1.6.2).



Σχήμα 1.6.1



Σχήμα 1.6.2

Ορισμός 1.4 Ορίζουμε τον πολλαπλασιασμό ενός φυσικού αριθμού με ένα σημείο ως

$$nP = P + P + \dots + P$$

n φορές.

Θεώρημα 1.2 Η πρόσθεση σημείων πάνω σε μία ελλειπτική καμπύλη ικανοποιεί τις παρακάτω ιδιότητες:

1. $P + \mathcal{O} = P$ (ουδέτερο στοιχείο).
2. $P + (-P) = \mathcal{O}$, όπου $P = (x, y)$ και $-P = (x, -y)$ (αντίθετο στοιχείο).
3. $P + (Q + R) = (P + Q) + R$, $P, Q, R \in \mathcal{E}$ (προσεταιριστική ιδιότητα).
4. $P + Q = Q + P$, $P, Q \in \mathcal{E}$ (μεταθετική ιδιότητα).

Τα σημεία της ελλειπτικής καμπύλης με πράξη την πρόσθεση σημείων όπως ορίστηκε παραπάνω αποτελούν *αβελιανή ομάδα*.

Απόδειξη Το $\mathcal{O}$ βρίσκεται σε κατακόρυφη ευθεία, συνεπώς οι αποδείξεις των ιδιοτήτων (1),(2) προκύπτουν εύκολα από τον ορισμό. Η απόδειξη της ιδιότητας (3) είναι αρκετά περίπλοκη και ο αναγνώστης μπορεί να ανατρέξει στο [27] για την απόδειξη της.

Για την ιδιότητα (4): Η ευθεία που διέρχεται από τα P, Q ταυτίζεται με την ευθεία που διέρχεται από τα Q, P . Επομένως, $P + Q = Q + P$, με $P, Q \in \mathcal{E}$.

1.3 Ισομορφισμοί και j - αναλλοίωτη Ελλειπτικής Καμπύλης

Ορισμός 1.5 Έστω δύο ελλειπτικές καμπύλες $\mathcal{E}_1, \mathcal{E}_2$ ορισμένες στο $\mathbb{F}$ με εξισώσεις

$$\begin{aligned}\mathcal{E}_1: y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6, \\ \mathcal{E}_2: y^2 + \bar{a}_1xy + \bar{a}_3y &= x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6.\end{aligned}$$

Οι $\mathcal{E}_1, \mathcal{E}_2$ λέγονται **ισόμορφες** πάνω από το $\mathbb{F}$ ($\mathcal{E}_1 \cong \mathcal{E}_2$) αν και μόνο αν υπάρχουν αριθμοί $u, r, s, t \in \mathbb{F}$, με $u \neq 0$ τέτοιοι ώστε η αλλαγή μεταβλητών

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

να μετατρέψει την εξίσωση της $\mathcal{E}_1$ στην εξίσωση της $\mathcal{E}_2$. Η σχέση του ισομορφισμού είναι μία σχέση ισοδυναμίας στο $\mathbb{F}$.

Έστω $\overline{\mathbb{F}}^\times$ η πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων του αλγεβρικά κλειστού σώματος $\mathbb{F}$ και έστω η ελλειπτική καμπύλη

$$\mathcal{E}: y^2 = x^3 + Ax + B$$

σε κανονική μορφή Weierstrass, όπου $A, B \in \mathbb{F}$, με χαρακτηριστική $\neq 2, 3$. Θέτουμε

$$x_1 = \mu^2 x \quad \text{και} \quad y_1 = \mu^3 y, \quad \text{όπου} \quad \mu \in \overline{\mathbb{F}}^\times.$$

Οπότε, προκύπτει

$$\mathcal{E}': y_1^2 = x_1^3 + A_1 x_1 + B_1, \quad \text{όπου} \quad A_1 = \mu^4 A \quad \text{και} \quad B_1 = \mu^6 B.$$

Παρατηρούμε ότι η νέα καμπύλη $\mathcal{E}'$ έχει την ίδια μορφή με την $\mathcal{E}$. Επομένως, από την αλλαγή μεταβλητών που πραγματοποιήσαμε προκύπτει μία ισόμορφη με την αρχική καμπύλη σε κανονική μορφή Weierstrass.

Η καμπύλη έχει διακρίνουσα $\Delta = -16(4A^3 + 27B^2)$ και εφόσον είναι ελλειπτική ισχύει $\Delta \neq 0$. Συνεπώς, έχουμε $4A^3 + 27B^2 \neq 0$. Τότε μπορούμε να ορίσουμε την ποσότητα

$$j(\mathcal{E}) = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

η οποία καλείται j - αναλλοίωτος (j - invariant) της ελλειπτικής καμπύλης $\mathcal{E}$. Όπως διαπιστώνουμε, η αλλαγή μεταβλητών που εφαρμόσαμε προηγουμένως αφήνει την ποσότητα $j(\mathcal{E})$ αμετάβλητη.

Θεώρημα 1.4 [23] Δύο ελλειπτικές καμπύλες ορισμένες πάνω από ένα αλγεβρικά κλειστό σώμα είναι **ισόμορφες** (ισοδύναμες) αν και μόνο αν έχουν την ίδια j -αναλλοίωτη.

Έστω $\overline{\mathbb{F}}$ ένα αλγεβρικό κάλυμμα του $\mathbb{F}$.

Έστω οι ελλειπτικές καμπύλες

$$\mathcal{E}_1: y_1^2 = x_1^3 + A_1 x_1 + B_1$$

και

$$\mathcal{E}_2: y_2^2 = x_2^3 + A_2 x_2 + B_2,$$

με j - αναλλοίωτα j_1 και j_2 αντίστοιχα. Αν $j_1 = j_2$, τότε υπάρχει $\mu \neq 0$, $\mu \in \overline{\mathbb{F}}$ τέτοιο ώστε

$$A_2 = \mu^4 A_1 \quad \text{και} \quad B_2 = \mu^6 B_1.$$

Χρησιμοποιούμε τον μετασχηματισμό

$$x_1 = \mu^2 x_2 \quad \text{και} \quad y_1 = \mu^3 y_2$$

για να φέρουμε σε ισοδύναμη μορφή τις δύο καμπύλες.

Απόδειξη Έστω $A_1 \neq 0$. Αυτό ισοδυναμεί με τη συνθήκη $j_1 \neq 0$ άρα και $A_2 \neq 0$. Επιλέγουμε μ , τέτοιο ώστε $A_2 = \mu^4 A_1$ και έχουμε:

$$\frac{4 A_2^3}{4 A_2^3 + 27 B_2^2} = \frac{4 A_1^3}{4 A_1^3 + 27 B_1^2} = \frac{4 \mu^{-12} A_2^3}{4 \mu^{-12} A_2^3 + 27 B_1^2} = \frac{4 A_2^3}{4 A_2^3 + 27 \mu^{12} B_1^2}.$$

Επομένως, $B_2^2 = (\mu^6 B_1)^2$ άρα $B_2 = \pm \mu^6 B_1$.

- Αν $B_2 = \mu^6 B_1$, η απόδειξη ολοκληρώθηκε.
- Αν $B_2 = -\mu^6 B_1$, τότε θέτουμε $\mu = i\mu$, όπου $i^2 = -1$. Αυτό δεν επηρεάζει τη σχέση $A_2 = \mu^4 A_1$ και έτσι καταλήγουμε ότι $B_2 = \mu^6 B_1$.
- Αν $A_1 = 0$, τότε προκύπτει ότι και $A_2 = 0$. Επίσης $4A_i^3 + 27B_i^2 \neq 0$, συνεπώς $B_1, B_2 \neq 0$. Οπότε, επιλέγουμε μ τέτοιο ώστε $B_2 = \mu^6 B_1$. $\square$

Υπάρχουν κάποιες ειδικές περιπτώσεις για το j .

1. Αν $j = 0$, η ελλειπτική καμπύλη $\mathcal{E}$ έχει τη μορφή

$$y^2 = x^3 + B.$$

2. Αν $j = 1728$, η ελλειπτική καμπύλη $\mathcal{E}$ έχει τη μορφή

$$y^2 = x^3 + Ax.$$

1.4 Εξισώσεις Ελλειπτικών Καμπυλών σε Διαφορετικές Μορφές

Στην παρούσα εργασία, οι ελλειπτικές καμπύλες βρίσκονται κυρίως σε μορφή Weierstrass. Ωστόσο, υπάρχουν εναλλακτικές μορφές ελλειπτικών καμπυλών χρήσιμες για την κρυπτογραφία που κρίνεται σκόπιμο να εξεταστούν.

1.4.1 Ελλειπτικές Καμπύλες Edwards

Οι καμπύλες Edwards είναι μια οικογένεια ελλειπτικών καμπυλών που μελετήθηκαν από τον Harold Edwards το 2007. [13] Η χρήση των καμπυλών Edwards στην κρυπτογραφία αναπτύχθηκε από τους Daniel J. Bernstein και Tanja Lange, οι οποίοι ανέδειξαν πληθώρα πλεονεκτημάτων της μορφής Edwards σε σύγκριση με την ευρύτερα χρησιμοποιούμενη μορφή Weierstrass.

Ορισμός 1.6 Η εξίσωση μιας καμπύλης Edwards πάνω από ένα σώμα $\mathbb{F}$, με χαρακτηριστική $\neq 2$ ($\text{char}(\mathbb{F}) \neq 2$) γράφεται:

$$x^2 + y^2 = 1 + dx^2y^2, \text{ όπου } d \in \mathbb{F} \setminus \{0, 1\}. \quad (1.4)$$

- Αν $d = 0$ η εξίσωση (1.4) περιγράφει τον μοναδιαίο κύκλο.
- Αν $d = 1$ η εξίσωση (1.4) περιγράφει τέσσερις ευθείες και συγκεκριμένα τις $x = \pm 1$ και $y = \pm 1$.

Συνεπώς, σε καμία από τις δύο αυτές περιπτώσεις, η αντίστοιχη καμπύλη δεν είναι ελλειπτική.

Επιπλέον, ως καμπύλη Edwards ορίζεται η καμπύλη που περιγράφεται από την παρακάτω εξίσωση, με παραμέτρους c, d

$$x^2 + y^2 = c^2(1 + dx^2y^2),$$

όπου $c, d \in \mathbb{F}$, με $cd(1 - c^4d) \neq 0$. [12]

Παράδειγμα 1.4 Στο παρακάτω σχήμα απεικονίζονται καμπύλες Edwards με εξίσωση

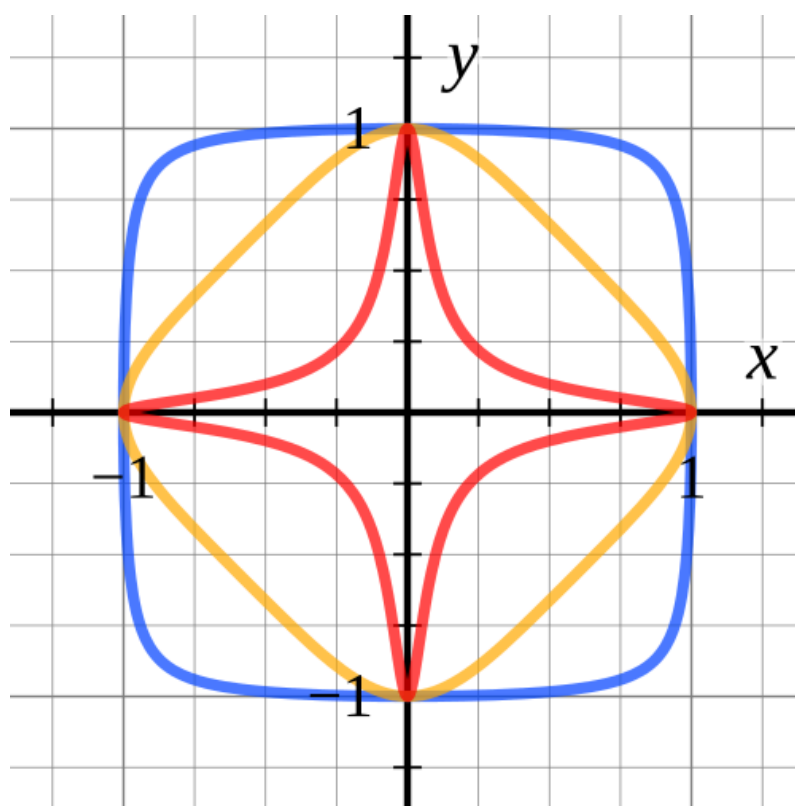
$$x^2 + y^2 = 1 + d x^2 y^2,$$

για διαφορετικές τιμές της παραμέτρου d .

Για $d = -300$ προκύπτει η κόκκινη γραφική παράσταση.

Για $d = -\sqrt{8}$ αντιστοιχεί η κίτρινη γραφική παράσταση.

Για $d = 0.9$ απεικονίζεται η μπλε γραφική παράσταση.



Σχήμα 1.7: Καμπύλες Edwards

1.4.2 Ελλειπτικές Καμπύλες Twisted Edwards

Οι ελλειπτικές καμπύλες Twisted Edwards (περιστρεφόμενες καμπύλες Edwards) αποτελούν μία γενίκευση των καμπυλών Edwards, οι οποίες εισήχθησαν από τους Bernstein, Birkner, Joye, Lange και Peters το 2008. Οι

ελλειπτικές καμπύλες Twisted Edwards κατέχουν καθοριστικό ρόλο στο σχήμα ψηφιακής υπογραφής EdDSA, καθώς επιτυγχάνει υψηλή αποδοτικότητα και παράλληλα αποφεύγει προβλήματα ασφαλείας που έχουν παρατηρηθεί σε άλλα σχήματα ψηφιακής υπογραφής.

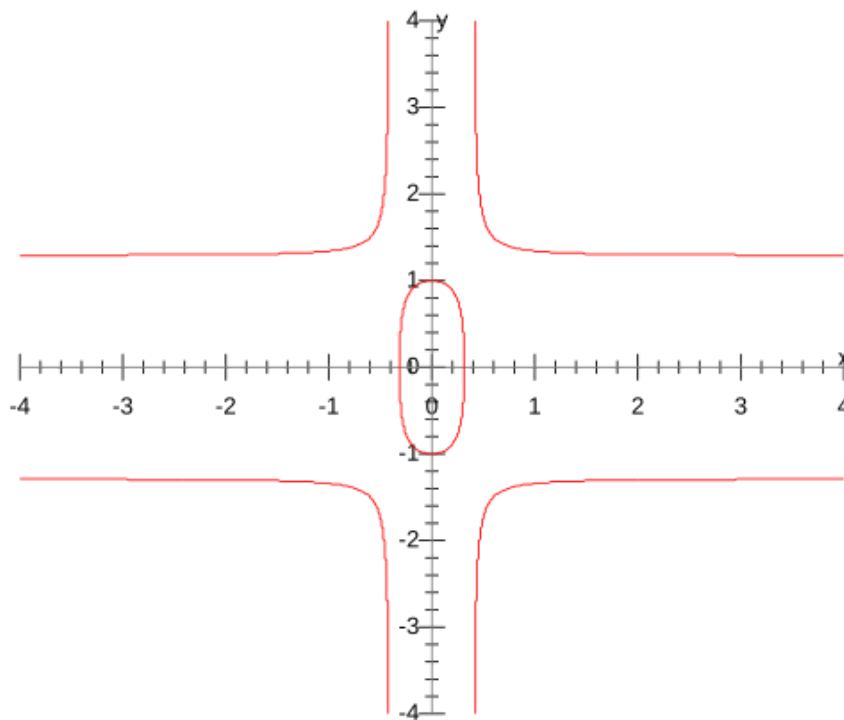
Ορισμός 1.7 Μία καμπύλη Twisted Edwards $\mathcal{E}_{E,a,d}$ πάνω από ένα σώμα $\mathbb{F}$, με χαρακτηριστική $\neq 2$ είναι μία επίπεδη καμπύλη που ορίζεται από την εξίσωση

$$\mathcal{E}_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

όπου τα a, d είναι διακριτά, μη-μηδενικά στοιχεία του $\mathbb{F}$. [6]

Μία καμπύλη Edwards είναι μία περιστρεφόμενη καμπύλη Edwards, για $a=1$.

Παράδειγμα 1.5 Περιστρεφόμενη ελλειπτική καμπύλη Edwards με εξίσωση $10x^2 + y^2 = 1 + 6x^2y^2$.



Εικόνα 1.8: Ελλειπτική καμπύλη Twisted Edwards

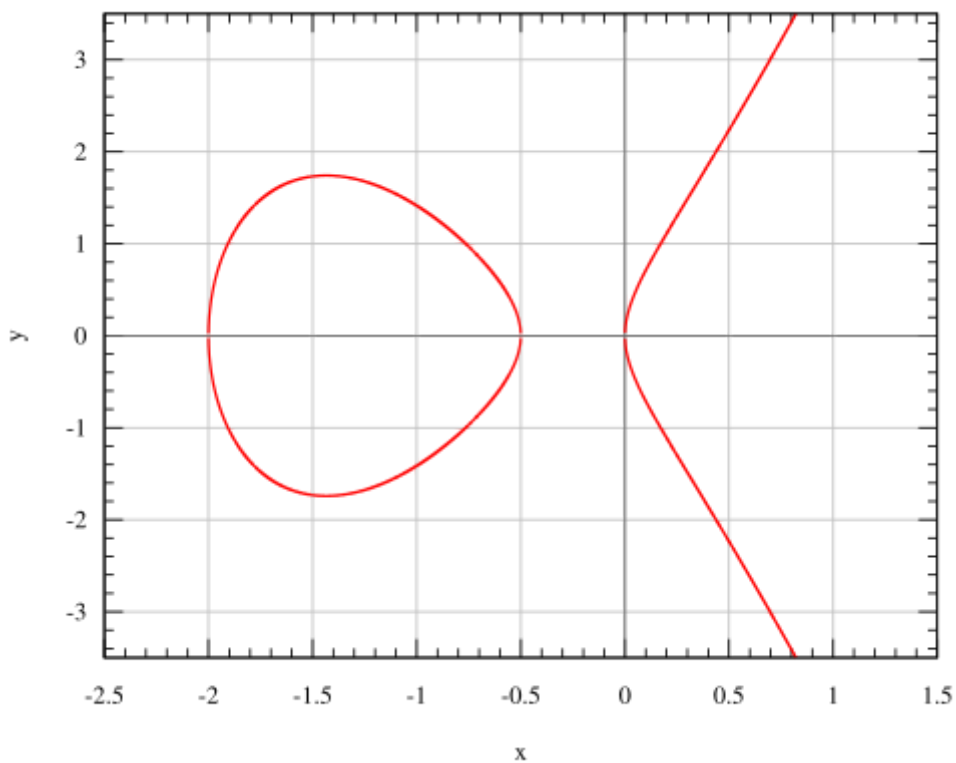
1.4.3 Ελλειπτικές Καμπύλες Montgomery

Η καμπύλη Montgomery αποτελεί μία μορφή ελλειπτικής καμπύλης, η οποία εισήχθη από τον Peter L. Montgomery το 1987. Εξαιτίας της ταχύτητας και της ασφάλειας που προσφέρει χρησιμοποιείται σε διάφορες κρυπτογραφικές εφαρμογές. [11]

Ορισμός 1.8 Μια καμπύλη Montgomery πάνω από ένα σώμα $\mathbb{F}$ ορίζεται από την εξίσωση

$$M_{A,B} : By^2 = x^3 + Ax^2 + x, \text{ όπου } A, B \in \mathbb{F} \text{ και } B(A^2 - 4) \neq 0.$$

Παράδειγμα 1.6 Καμπύλη Montgomery με εξίσωση $\frac{1}{4}y^2 = x^3 + \frac{5}{2}x^2 + x$.



Σχήμα 1.9 Καμπύλη Montgomery

1.4.4 Ελλειπτικές Καμπύλες στη Μορφή του Legendre

Ορισμός 1.9 Έστω ένα σώμα $\mathbb{F}$, με χαρακτηριστική $\neq 2$ και έστω

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$$

μία ελλειπτική καμπύλη $\mathcal{E}$ πάνω στο $\mathbb{F}$, με $e_1, e_2, e_3 \in \mathbb{F}$.

$$\begin{aligned} \text{Έστω} \quad x_1 &= (e_2 - e_1)^{-1}(x - e_1), \\ y_1 &= (e_2 - e_1)^{-3/2}y, \\ \lambda &= \frac{e_3 - e_1}{e_2 - e_1}. \end{aligned}$$

Τότε $\lambda \neq 0, 1$ και

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda). \quad [23]$$

Απόδειξη Προκύπτει άμεσα με απλούς υπολογισμούς.

Η παράμετρος λ για την ελλειπτική καμπύλη $\mathcal{E}$ δεν είναι μοναδική. Καθένα από τα στοιχεία του παρακάτω συνόλου

$$\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}$$

οδηγεί σε μια εξίσωση Legendre για την καμπύλη $\mathcal{E}$. Οι περιπτώσεις αυτές αντιστοιχούν σε έξι μεταθέσεις των ριζών e_1, e_2, e_3 . Αυτές είναι οι μοναδικές τιμές της παραμέτρου λ που αντιστοιχούν στην καμπύλη $\mathcal{E}$, οπότε η απεικόνιση $\lambda \mapsto \mathcal{E}$ είναι εξαπλή, εκτός από τις περιπτώσεις όπου

$$\lambda = -1, 1/2, 2, \quad \text{ή όπου} \quad \lambda^2 - \lambda + 1 = 0.$$

Στις περιπτώσεις αυτές, το παραπάνω σύνολο εκφυλίζεται. [28]

1.4.5 Ελλειπτικές Καμπύλες του Hesse

Στη γεωμετρία, η καμπύλη του Hesse είναι μία κυβική επίπεδη καμπύλη, η οποία παρουσιάζει ομοιότητες με το “φύλλο” του Descartes. Η ονομασία της προέρχεται από τον Γερμανό μαθηματικό Otto Hesse. Οι συγκεκριμένες καμπύλες αξιοποιούνται στην κρυπτογραφία ελλειπτικών καμπυλών, καθώς η εκτέλεση αριθμητικών πράξεων είναι ταχύτερη και απαιτεί λιγότερη μνήμη σε σχέση με την κλασική μορφή Weierstrass.

Έστω $\mathbb{F}$ σώμα με $\text{char}(\mathbb{F}) > 3$.

Ορισμός 1.10 Η Hessian κυβική ελλειπτική καμπύλη πάνω από το $\mathbb{F}$ είναι μια καμπύλη με εξίσωση της μορφής

$$\mathcal{E}_D(\mathbb{F}) : u^3 + v^3 + 1 = 3Duv, \quad \text{με } D \in \mathbb{F} \text{ και } D^3 \neq 1.$$

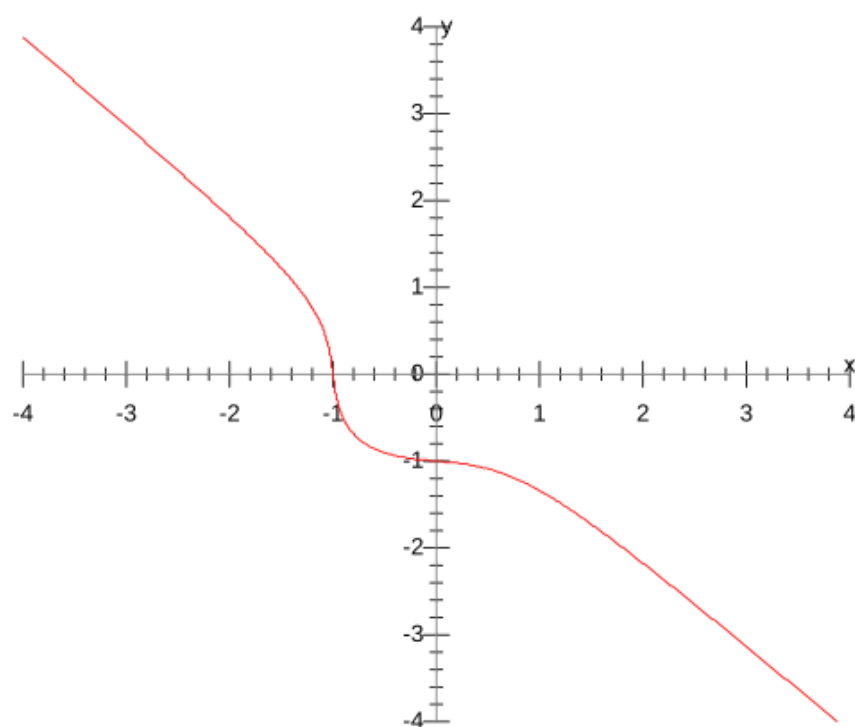
Με τη συνθήκη $D^3 \neq 1$ εξασφαλίζεται η ομαλότητα της καμπύλης, δηλαδή ότι η καμπύλη είναι ελλειπτική (μη ιδιάζουσα). Έτσι, προκύπτει το παρακάτω λήμμα. [14]

Λήμμα Μια Hessian κυβική καμπύλη είναι *ιδιάζουσα* αν και μόνο αν $D^3 = 1$.

Απόδειξη Για την απόδειξη του παραπάνω λήμματος, ανατρέξτε στο [14].

Παράδειγμα 1.7 Ελλειπτική καμπύλη Hessian με εξίσωση

$$x^3 + y^3 + 1 = 0.3xy$$



Σχήμα 1.10: Ελλειπτική καμπύλη *Hessian*

Κεφάλαιο 2

Ελλειπτικές Καμπύλες επί πεπερασμένων σωμάτων

Σε αυτό το κεφάλαιο θα μελετήσουμε τις ελλειπτικές καμπύλες ορισμένες σε πεπερασμένα σώματα και θα δώσουμε μια απόδειξη του Θεωρήματος του Hasse.

2.1 Ελλειπτικές καμπύλες ορισμένες πάνω από Πεπερασμένα σώματα

Οι ελλειπτικές καμπύλες οι οποίες παρουσιάζουν ιδιαίτερο κρυπτογραφικό ενδιαφέρον είναι ορισμένες στο σώμα $\mathbb{F}_q$, όπου q πρώτος.

Έστω $\mathbb{F}_q$ το πεπερασμένο σώμα με q στοιχεία. Επίσης, έστω μια ελλειπτική καμπύλη E σε κανονική μορφή Weierstrass πάνω σε ένα πεπερασμένο σώμα $\mathbb{F}_q$, όπου q πρώτος της μορφής

$$y^2 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6, \quad (2.1)$$

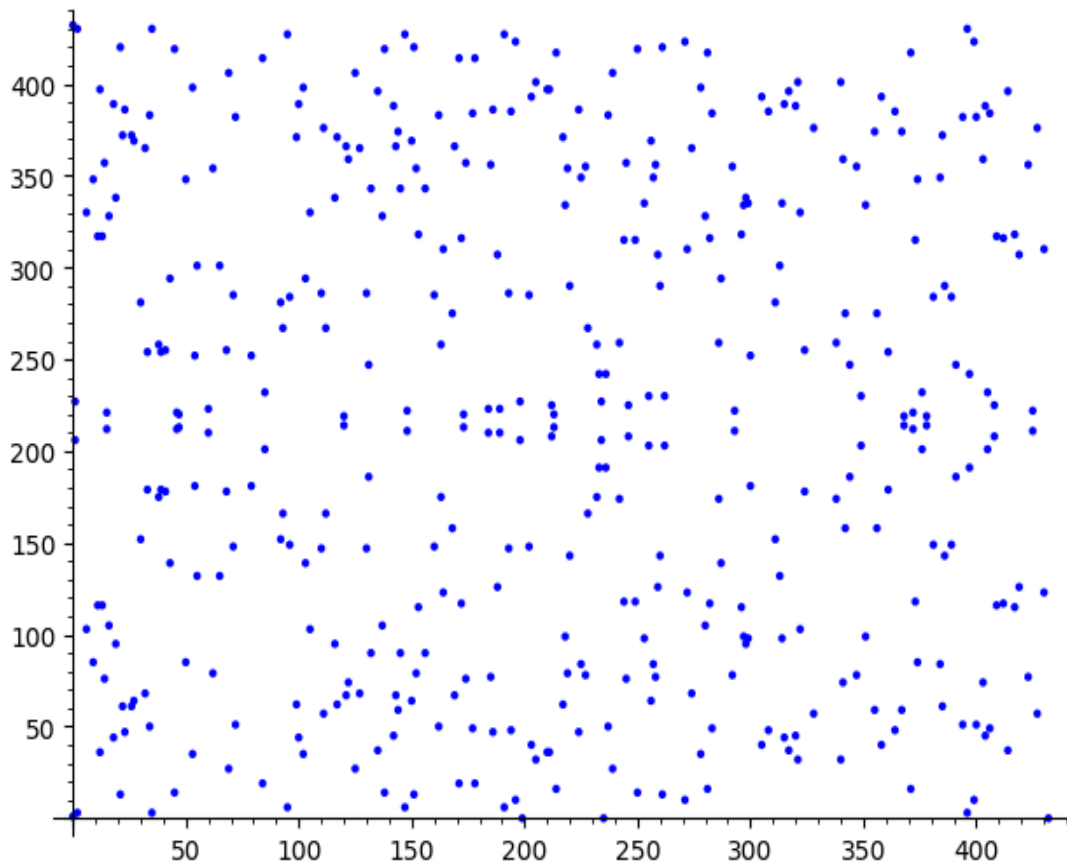
όπου $\alpha_2, \alpha_4, \alpha_6 \in \mathbb{F}_q$. Τότε το σύνολο των σημείων της E με συντεταγμένες στο $\mathbb{F}_q$ είναι το σύνολο

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q : y^2 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6\} \cup \{\mathcal{O}\}.$$

Παρατηρούμε ότι μια τέτοια ελλειπτική καμπύλη μπορεί να έχει το πολύ $2q + 1$

σημεία, το σημείο $\mathcal{O}$ μαζί με $2q$ ζεύγη (x, y) , $x, y \in \mathbb{F}_q$, που ικανοποιούν την εξίσωση (2.1). Αυτό συμβαίνει επειδή για κάθε ένα από τα q πιθανά x υπάρχουν το πολύ δύο y ώστε να ικανοποιείται η εξίσωση της ελλειπτικής καμπύλης. Εκτιμάται ότι υπάρχουν περίπου τα μισά από αυτά τα $2q + 1$ σημεία στην καμπύλη, καθώς τετραγωνική ρίζα έχουν μόνο τα μισά από τα στοιχεία του $\mathbb{F}_q^*$. [2]

Παράδειγμα 2.1 Ελλειπτική καμπύλη με εξίσωση $\mathcal{E}: y^2 = x^3 + 1$ στο $\mathbb{F}_{433}$. [22]



Σχήμα 2.1 : $\mathcal{E}: y^2 = x^3 + 1$ στο $\mathbb{F}_{433}$

2.2 Θεώρημα Hasse

Για την κατασκευή ενός κρυπτοσυστήματος που βασίζεται σε ελλειπτική καμπύλη είναι κρίσιμο να γνωρίζουμε την τάξη της ομάδας, δηλαδή το πλήθος των σημείων μιας ελλειπτικής καμπύλης. Όσο μεγαλύτερος είναι ο αριθμός των σημείων μιας καμπύλης τόσο μεγαλύτερη θα είναι και η εξαντλητική αναζήτηση.

Θεώρημα Hasse. Ας είναι $\text{char}(\mathbb{F}_q) \geq 3$, και $\mathcal{E}$ η ελλειπτική καμπύλη η οποία ορίζεται από την εξίσωση

$$y^2 = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$$

όπου $\alpha_2, \alpha_4, \alpha_6 \in \mathbb{F}_q$. Τότε το πλήθος των σημείων της $\mathcal{E}$ πάνω από το $\mathbb{F}_q$, $\#\mathcal{E}(\mathbb{F}_q)$ ικανοποιεί την ανίσωση

$$\left| \#\mathcal{E}(\mathbb{F}_q) - (q + 1) \right| \leq 2\sqrt{q}.$$

Στη συνέχεια, θα δοθεί μία απόδειξη του Θεωρήματος του Hasse.

Το θεώρημα του Hasse δίνει ένα φράγμα για τον πληθάρημο του $\mathcal{E}(\mathbb{F}_q)$ αλλά δεν δίνει έναν τρόπο υπολογισμού αυτού. Ο ακριβής υπολογισμός της ποσότητας $\#\mathcal{E}(\mathbb{F}_q)$ είναι πιο δύσκολος. Τη λύση στο πρόβλημα αυτό έδωσε το 1985 ο Schoof με τη σχεδίαση ενός αλγορίθμου. Πρόκειται για έναν αλγόριθμο χρονικής πολυπλοκότητας $O((\log)^8)$, ο οποίος έχει πρακτική εφαρμογή για πρώτους p αρκετών εκατοντάδων ψηφίων. [2] Στη συνέχεια, οι Elkies, Morain, Atkin κ.α βελτίωσαν αυτόν τον αλγόριθμο και πλέον είναι σε θέση να μπορεί να υπολογίσει τον πληθάρημο μέσα σε μερικά λεπτά. Αυτή η βελτιωμένη εκδοχή του αλγορίθμου είναι γνωστή ως ο αλγόριθμος SEA. [23]

Απόδειξη Θεωρήματος Hasse. Για την απόδειξη αυτού του θεωρήματος θεωρούμε ότι:

- $q = p^r$, για κάποιον πρώτο αριθμό p , με $p \neq 2$ και $r \in \mathbb{N}$,
- $K = \mathbb{F}_q(t)$, το σώμα συναρτήσεων ως προς t πάνω από το $\mathbb{F}_q$.

Έστω οι ελλειπτικές καμπύλες $\mathcal{E}_1, \mathcal{E}_2$ ορισμένες πάνω από ένα σώμα K . Τότε η $\mathcal{E}_1$ αποτελεί μία *συστροφή* της $\mathcal{E}_2$ πάνω στο K , αν οι $\mathcal{E}_1, \mathcal{E}_2$ είναι *ισόμορφες* πάνω σε μία πεπερασμένη επέκταση L του K . Έστω $K = \mathbb{F}_p(x)$ το σώμα συναρτήσεων μίας μεταβλητής πάνω στο $\mathbb{F}_p$, και έστω η ελλειπτική καμπύλη $\mathcal{E}$, η οποία περιγράφεται από μια εξίσωση της μορφής

$$\mathcal{E}: Y^2 = X^3 + aX + b. \quad (2.2)$$

Αν $\mathcal{E}_\lambda$ είναι η ελλειπτική καμπύλη της μορφής

$$\lambda Y^2 = X^3 + aX + b, \quad (2.3)$$

όπου

$$\lambda = \lambda(x) = x^3 + ax + b,$$

τότε οι καμπύλες $\mathcal{E}$, $\mathcal{E}_\lambda$ ορίζονται πάνω στο K και η $\mathcal{E}_\lambda$ αποτελεί μία συστροφή της $\mathcal{E}$ πάνω στο K .

Στη συνέχεια, θεωρούμε την ομάδα $\mathcal{E}_\lambda(K)$ των K -ρητών σημείων της $\mathcal{E}_\lambda$. Αν τα σημεία (X, Y) , $(X_j, Y_j) \in \mathcal{E}_\lambda(\mathcal{E})$, $j = 1, 2$, με

$$(X, Y) = (X_1, Y_1) + (X_2, Y_2), \text{ τότε}$$

$$X = \lambda \left(\frac{Y_1 - Y_2}{X_1 - X_2} \right)^2 - (X_1 + X_2). \quad (2.4)$$

Αν $(X, Y) = 2(X_1, Y_1)$, τότε

$$X = \frac{(3X_1^2 + a)^2}{4(X_1^3 + aX_1 + b)\lambda} - 2X_1$$

Στο σώμα $K = \mathbb{F}_p(x)$, η εξίσωση (2.3) έχει δύο προφανείς λύσεις, οι οποίες είναι

$$(x, 1), (x_0, -1) = -(x_0, 1).$$

Μία λιγότερο προφανής λύση είναι η

$$X_0 = x^p, \quad Y_0 = (x^3 + ax + b)^{(p-1)/2}.$$

Έστω

$$(X_n, Y_n) = (X_0, Y_0) + n(x, 1), \quad n \in \mathbb{Z}.$$

Αν $(X_n, Y_n) \neq 0$, θα δείξουμε ότι $X_n \neq 0$. Γράφουμε το X_n σε ανάγωγη μορφή, ως $X_n = P_n / Q_n$, με $Q_n, P_n \in \mathbb{F}_p[x]$, όπου το P_n είναι μονικό, δηλαδή ο συντελεστής του μεγιστοβάθμιου όρου ισούται με 1. Έχουμε μία καλά ορισμένη συνάρτηση

$$d: \mathbb{Z} \rightarrow \{0, 1, 2, 3, \dots\},$$

η οποία δίνεται από τον τύπο

$$d(n) = d_n = 0, \text{ αν } (X_n, Y_n) = 0,$$

και

$$d(n) = d_n = \deg(P_n), \text{ αλλιώς.}$$

Η απόδειξη του Manin για το Θεώρημα του Hasse βασίζεται στην ακόλουθη βασική ταυτότητα (Basic Identity):

$$\text{Basic Identity:} \quad d_{n-1} + d_{n+1} = 2d_n + 2.$$

Ο αναγνώστης παραπέμπεται στο [26] για την απόδειξη της ταυτότητας.

Η σύνδεση μεταξύ του Θεωρήματος του Hasse και της συνάρτησης $d(n)$ επιτυγχάνεται μέσω της ακόλουθης σχέσης:

$$d_{-1} - d_0 - 1 = N_p - p. \quad (2.5)$$

Για την απόδειξη της σχέσης (2.5) θα χρειαστεί να απλοποιήσουμε τη ρητή συνάρτηση X_{-1} . Με τη βοήθεια του τύπου της πρόσθεσης (2.4) προκύπτει ότι:

$$\begin{aligned} X_{-1} &= \frac{(x^3 + ax + b)[(x^3 + ax + b)^{(p-1)/2} + 1]^2}{(x^p - x)^2} - (x^p + x) \\ &= \frac{x^{2p+1} + R(x)}{(x^p - x)^2}, \end{aligned}$$

όπου το $R(x)$ είναι πολυώνυμο βαθμού το πολύ $2p$. Για την παραγοντοποίηση του X_{-1} στη μορφή P_{-1} / Q_{-1} θα χρησιμοποιήσουμε τη σχέση:

$$(x^p - x) = x(x - 1) \cdot \cdots \cdot (x - p + 1).$$

Οι μόνοι παράγοντες που απαλείφονται από τον παρονομαστή είναι είτε ο όρος $(x - r)^2$ με το σύμβολο του Legendre

$$\left(\frac{r^3 + ar + b}{p}\right) = (r^3 + ar + b)^{(p-1)/2} = -1,$$

είτε ο παράγοντας $x - r$, με $r^3 + ar + b = 0$ ($0 \leq r < p$). Αν m είναι το πλήθος των παραγόντων της πρώτης περίπτωσης και n ο αριθμός των παραγόντων της δεύτερης περίπτωσης, τότε

$$d_{-1} = \deg P_{-1} = 2p + 1 - 2m - n.$$

Όμως, $d_0 = p$, οπότε

$$d_{-1} - d_0 = p + 1 - 2m - n. \quad (2.6)$$

Κάθε r στο $\mathbb{F}_p$, με $r^3 + ar + b \neq 0$ και

$$\left(\frac{r^3 + ar + b}{p}\right) = 1$$

θα δώσει δύο λύσεις της εξίσωσης (2.2), ενώ η εξίσωση $r^3 + ar + b = 0$ δίνει μία μόνο λύση. Συνεπώς,

$$N_p = 2(p - m) - n$$

και η σχέση (2.5) προκύπτει από την (2.6).

Λήμμα Η συνάρτηση $d(n)$ είναι ένα τετραγωνικό πολυώνυμο στο n . Πράγματι,

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0.$$

Απόδειξη Για $n = -1, 0$, το παραπάνω λήμμα είναι προφανές ότι ισχύει. Υποθέτουμε ότι είναι αληθές για $n - 1$ και n ($n \geq 0$). Από τη βασική ταυτότητα,

$$\begin{aligned} d_{n+1} &= 2d_n - d_{n-1} + 2 \\ &= 2[n^2 - (d_{-1} - d_0 - 1)n + d_0] \end{aligned}$$

$$\begin{aligned}
& - [(n - 1)^2 - (d_{-1} - d_0 - 1)(n - 1) + d_0] + 2 \\
& = (n + 1)^2 - (d_{-1} - d_0 - 1)(n + 1) + d_0,
\end{aligned}$$

αποδεικνύεται το λήμμα για $n + 1$. Μέσω επαγωγής καταλήγουμε στο συμπέρασμα ότι το λήμμα ισχύει για κάθε $n \geq -1$. Με τον ίδιο τρόπο, το λήμμα ισχύει για κάθε $n \leq 0$. $\square$

Συνεχίζουμε την απόδειξη του Θεωρήματος του Hasse και έχουμε ότι το τετραγωνικό πολυώνυμο

$$\begin{aligned}
d(x) &= x^2 - (d_{-1} - d_0 - 1)x + d_0 \\
&= x^2 - (N_p - p)x + d_0
\end{aligned}$$

λαμβάνει μη αρνητικές τιμές, για κάθε $n \in \mathbb{Z}$. Επομένως, η διακρίνουσα του

$$D = (N_p - p)^2 - 4p$$

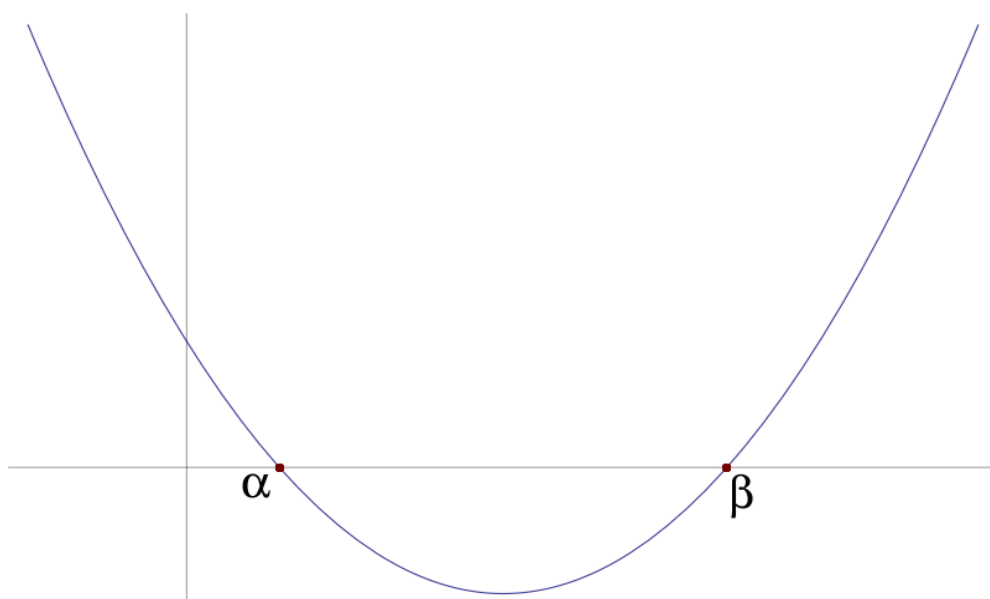
δε μπορεί να είναι θετική, γιατί διαφορετικά το πολυώνυμο $d(x)$ θα είχε δύο πραγματικές ρίζες α, β , έτσι ώστε για κάποιο n να ισχύει:

$$n \leq \alpha < \beta \leq n + 1.$$

Συνεπώς, είναι αδύνατο να ισχύουν ταυτόχρονα και οι δύο ισότητες, καθώς η $d(n)$ δεν μπορεί να μηδενιστεί ταυτόχρονα για δύο διαδοχικούς ακέραιους. Αυτό είναι άτοπο, επειδή $(\alpha - \beta)^2 = D \in \mathbb{Z}$. Επομένως,

$$(N_p - p)^2 - 4p \leq 0,$$

το οποίο ολοκληρώνει την απόδειξη του Θεωρήματος του Hasse. [8] $\square$



Σχήμα 2.2 : Γραφική παράσταση της περίπτωσης $D > 0$

Κεφάλαιο 3

Κρυπτογραφικές Εφαρμογές

Στο κεφάλαιο αυτό ορίζεται το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες και παρουσιάζονται κάποιοι βασικοί κρυπτογραφικοί αλγόριθμοι, οι οποίοι βασίζονται στην κρυπτογράφηση με τη χρήση των ελλειπτικών καμπυλών.

3.1 Πρόβλημα Διακριτού Λογαρίθμου για Ελλειπτικές Καμπύλες

Έστω μια ελλειπτική καμπύλη E , η οποία είναι ορισμένη στο πεπερασμένο σώμα $\mathbb{F}_p$ και $P \in E(\mathbb{F}_p)$ ένα σημείο της. Θεωρούμε το σημείο $Q \in \langle P \rangle$, δηλαδή ανήκει στην υποομάδα που παράγεται από το P . Τότε ως πρόβλημα διακριτού λογαρίθμου στις ελλειπτικές καμπύλες (ECDLP) ορίζεται το εξής: Αν

$$Q = nP$$

ζητείται να βρεθεί ο ακέραιος n , όπου $n \in \{1, \dots, \text{ord}(P) - 1\}$. Το πρόβλημα αυτό ορίζεται σε κάθε αβελιανή ομάδα G . [1]

3.2 Κωδικοποίηση κειμένου σε Ελλειπτική Καμπύλη

Στην παράγραφο αυτή, θα δούμε έναν αποδοτικό αλγόριθμο, ο οποίος αντιστοιχεί μηνύματα κειμένου σε σημεία της ελλειπτικής καμπύλης E : $y^2 = x^3 + ax + b$ ορισμένη πάνω στο $\mathbb{F}_p$. Έστω οι ακέραιοι k, M , με $30 \leq k \leq 50$ και $kM < p$. Ορίζουμε το χώρο κειμένου ως το σύνολο

$$P = \{m \in \mathbb{Z} \mid 0 \leq m < M\}.$$

Δοθέντος ενός μηνύματος m υπολογίζουμε

$$x_j = km + j, \text{ για } j = 1, \dots, 30.$$

Στη συνέχεια, χρησιμοποιούμε το σύμβολο του Legendre για να ελέγξουμε αν η ποσότητα

$$x_j^3 + ax_j + b$$

αποτελεί τετραγωνικό υπόλοιπο *modulo* p . Σε αυτήν την περίπτωση, υπολογίζουμε επίσης, το $y_j \in \mathbb{F}_p$ έτσι ώστε

$$P_j = (x_j, y_j) \in \mathcal{E}(\mathbb{F}_p).$$

Συνεπώς, το μήνυμα m αντιστοιχήθηκε στο σημείο P_j της ελλειπτικής καμπύλης.

Για να μετατρέψουμε ένα σημείο P_j της ελλειπτικής καμπύλης στο αρχικό μήνυμα m , αρκεί να υπολογίσουμε:

$$\left[\frac{x_j - 1}{k} \right] = \left[\frac{k m + j - 1}{k} \right] = \left[m + \frac{j - 1}{k} \right] = m.$$

Θα πρέπει να υπάρχει τουλάχιστον μία τιμή y_j , όπου $j \in \{1, \dots, k\}$, έτσι ώστε το σημείο (x_j, y_j) να ανήκει στη ελλειπτική καμπύλη $\mathcal{E}(\mathbb{F}_p)$ προκειμένου η αντιστοίχιση να είναι επιτυχής.

Η πιθανότητα επιτυχίας για κάθε j ισούται με $|\mathcal{E}(\mathbb{F}_p)| / 2p$ και τείνει στο $1/2$. Επομένως, για k περιπτώσεις η πιθανότητα αποτυχίας είναι $1 / 2^k$, ενώ ως πιθανότητα επιτυχίας είναι ο αριθμός $1 - 1 / 2^k$. [20]

3.3 Πρωτόκολλο Ανταλλαγής Κλειδιού Diffie Hellman σε Ελλειπτικές Καμπύλες

Οι χρήστες A , B επιθυμούν να συμφωνήσουν σε ένα κοινό κλειδί, το οποίο θα χρησιμοποιήσουν αργότερα για την ανταλλαγή μηνυμάτων, χωρίς κάποιος τρίτος να μπορεί να το υπολογίσει. Τη λύση στο πρόβλημα αυτό δίνει ο αλγόριθμος Diffie - Hellman. Αρχικά, συμφωνούν σε ένα μεγάλο πρώτο αριθμό p και σε μία ελλειπτική καμπύλη $\mathcal{E}$ της μορφής

$$y^2 = x^3 + ax + b$$

ορισμένη στο $\mathbb{F}_p$, έτσι ώστε το πρόβλημα του διακριτού λογαρίθμου να είναι δύσκολο στο $\mathcal{E}(\mathbb{F}_p)$. Επίσης, αποφασίζουν από κοινού σε ένα σημείο βάσης P της ελλειπτικής καμπύλης $\mathcal{E}$. [20] Η υποομάδα που παράγεται από το P πρέπει να έχει μεγάλη τάξη. Συνήθως, η ελλειπτική καμπύλη και το σημείο

επιλέγονται ώστε η τάξη της υποομάδας να είναι ένας μεγάλος πρώτος αριθμός. [28]

Πρωτόκολλο Ανταλλαγής Κλειδιού Diffie - Hellman [20]

1. Ο χρήστης A επιλέγει έναν τυχαίο ακέραιο n_A και υπολογίζει $Q_A = n_A P$.
2. Ο χρήστης A κρατάει μυστικό το n_A και στέλνει το Q_A στον B.
3. Ο χρήστης B επιλέγει έναν τυχαίο ακέραιο n_B και υπολογίζει $Q_B = n_B P$.
4. Ο χρήστης B κρατάει μυστικό το n_B και στέλνει το Q_B στον A.
5. Ο χρήστης A υπολογίζει $n_A Q_B$.
6. Ο χρήστης B υπολογίζει $n_B Q_A$.

Συνεπώς, οι χρήστες A,B κατέληξαν να υπολογίζουν το ίδιο κοινό κλειδί, το οποίο γνωρίζουν μόνο οι ίδιοι

$$K = (n_A n_B)P,$$

καθώς πραγματοποίησαν τους ίδιους υπολογισμούς:

$$n_A Q_B = (n_A n_B)P,$$

$$n_B Q_A = (n_A n_B)P.$$

Επομένως, κάποιος που επιθυμεί να μάθει το κοινό κλειδί K θα χρειαστεί να λύσει το ακόλουθο πρόβλημα.

Πρόβλημα Diffie - Hellman σε Ελλειπτικές Καμπύλες:

Δοθέντος των σημείων P , $Q_A = n_A P$ και $Q_B = n_B P$ της $\mathcal{E}$ καλείται να υπολογίσει το σημείο $(n_A n_B) P$, όπου οι ακέραιοι n_A, n_B δεν είναι γνωστοί.

Αν κάποιος θα μπορούσε να επιλύσει το πρόβλημα του διακριτού λογαρίθμου στο $\mathcal{E}(\mathbb{F}_p)$, τότε θα μπορούσε να χρησιμοποιήσει το P και το $n_A P$ για να ανακαλύψει το μυστικό κλειδί του A. Έπειτα, θα μπορούσε να υπολογίσει το $n_B P$ και να φτάσει στο κλειδί K.

Για περισσότερες πληροφορίες, ο αναγνώστης παραπέμπεται στα [20] , [28].

3.4 Κρυπτοσύστημα ElGamal Ελλειπτικών Καμπυλών

Για τη δημιουργία ενός κρυπτοσυστήματος ελλειπτικών καμπυλών ανάλογο του κρυπτοσυστήματος ElGamal, ένας χρήστης A καλείται να επιλέξει έναν *μεγάλο πρώτο αριθμό* p και μία *ελλειπτική καμπύλη* E ορισμένη πάνω στο σώμα $\mathbb{F}_p$. Η ελλειπτική καμπύλη E έχει τη μορφή

$$y^2 = x^3 + ax + b.$$

Στη συνέχεια, ο χρήστης A επιλέγει ένα σημείο P της ελλειπτικής καμπύλης E και διαλέγει έναν *τυχαίο ακέραιο* n . Έπειτα, υπολογίζει το σημείο

$$Q = nP.$$

Η τετράδα (p, E, P, Q) αποτελεί το δημόσιο κλειδί του χρήστη A , ενώ ο ακέραιος n αντιπροσωπεύει το ιδιωτικό κλειδί.

Ο χρήστης B για να στείλει ένα σημείο - μήνυμα $M \in E(\mathbb{F}_p)$ στο χρήστη A , διαλέγει έναν *τυχαίο ακέραιο* k και υπολογίζει

$$C_1 = kP \quad \text{και} \quad C_2 = M + kQ.$$

Έτσι, προκύπτει το κρυπτοκείμενο (C_1, C_2) , το οποίο ο B το αποστέλλει στον A .

Για την αποκρυπτογράφηση του (C_1, C_2) , ο A υπολογίζει

$$C_2 - nC_1 = (M + kQ) - n(kP) = M + kQ - kQ = M.$$

Η ασφάλεια του ιδιωτικού κλειδιού βασίζεται στη δυσκολία υπολογισμού του διακριτού λογαρίθμου πάνω στην ελλειπτική καμπύλη E . Αν κάποιος καταφέρει να υπολογίσει το n , τότε θα μπορεί να διαβάσει όλα τα μηνύματα που λαμβάνει ο A . Αξίζει να σημειωθεί ότι, αν καταφέρει να υπολογίσει το k , τότε θα είναι σε θέση να υπολογίσει και το $C_2 - kQ = M$, οπότε θα διαβάσει το μήνυμα M . Για αυτό το λόγο, ο ακέραιος k θα πρέπει να κρατηθεί μυστικός.

Μειονέκτημα αποτελεί το γεγονός ότι το κρυπτοκείμενο που προκύπτει αποτελείται από ένα ζεύγος σημείων της καμπύλης E , το οποίο αντιστοιχεί σε τέσσερα στοιχεία του $\mathbb{Z}_p$. Συνεπώς, ένα σημείο $P = (x_p, y_p)$, το οποίο βρίσκεται

πάνω στην καμπύλη E μπορεί να περιγραφεί από το x_p και από ένα δυαδικό ψηφίο e_p , όπου

➤ Αν $0 \leq y_p < p/2$, τότε $e_p = 0$.

➤ Αν $p/2 < y_p < p$, τότε $e_p = 1$.

Η παραπάνω αναπαράσταση για το P ονομάζεται *συμπίεση σημείου (point compression)*. [20]

Παράδειγμα 3.1 Ο χρήστης A επιλέγει και δημοσιοποιεί την ελλειπτική καμπύλη E : $y^2 = x^3 + x + 6$ ορισμένη στο $\mathbb{F}_{11}$ και το σημείο $P = (2, 7)$ της ελλειπτικής καμπύλης E .

Στη συνέχεια, ο χρήστης A επιλέγει το ιδιωτικό κλειδί $n = 7$ και υπολογίζει το σημείο

$$Q = nP = 7(2, 7) = (7, 2).$$

Η τετράδα $(11, E, P, Q)$ αποτελεί το δημόσιο κλειδί του A .

Ο χρήστης B θέλει να στείλει το μήνυμα $M = (10, 9)$. Αρχικά, επιλέγει έναν τυχαίο ακέραιο $k = 3$ και υπολογίζει

$$C_1 = kP = 3(2, 7) = (8, 3),$$

$$C_2 = M + kQ = (10, 9) + 3(7, 2) = (10, 9) + (3, 5) = (10, 2).$$

Έτσι, προκύπτει το κρυπτοκείμενο (C_1, C_2) , το οποίο ο B στέλνει στον A .

Για την αποκρυπτογράφηση του μηνύματος, ο A υπολογίζει

$$C_2 - nC_1 = (10, 2) - 7(8, 3) = (10, 2) - (3, 5) = (10, 2) + (3, 6) = (10, 9)$$

και προκύπτει το αρχικό μήνυμα M .

3.5 Κρυπτοσύστημα Menezes - Vanstone Ελλειπτικής Καμπύλης

Στο κρυπτοσύστημα Menezes - Vanstone τα κείμενα (plaintexts) και τα κρυπτοκείμενα (ciphertexts) αποτελούν στοιχεία του $\mathbb{F}_p^* \times \mathbb{F}_p^*$ και ο ρόλος της

ελλειπτικής καμπύλης σε αυτήν την περίπτωση είναι να αποκρύπτει το μήνυμα.

Ο χρήστης A διαλέγει έναν πρώτο αριθμό $p > 3$, μία ελλειπτική καμπύλη E ορισμένη στο $\mathbb{F}_p$, ένα τυχαίο σημείο $P \in E(\mathbb{F}_p)$ και έναν ακέραιο αριθμό a . Έπειτα, υπολογίζει

$$Q = aP.$$

Η τετράδα (p, E, P, Q) αποτελεί το δημόσιο κλειδί και ο ακέραιος αριθμός a αντιπροσωπεύει το ιδιωτικό κλειδί του χρήστη A.

Ο χρήστης B χρησιμοποιεί το δημόσιο κλειδί του χρήστη A για να κρυπτογραφήσει το μήνυμα

$$(m_1, m_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$$

και να το στείλει στον A. Στη συνέχεια, ο χρήστης A διαλέγει τυχαίο ακέραιο $k \in \{0, \dots, \text{ord}(P) - 1\}$ και υπολογίζει:

1. $kQ = (y_1, y_2)$.
2. $kP = C_0$.
3. $c_j = y_j m_j \pmod{p}$, $j = 1, 2$

Έπειτα, ο B στέλνει στον A το κρυπτοκείμενο $C = (C_0, c_1, c_2)$.

Ο χρήστης A για να αποκρυπτογραφήσει το μήνυμα χρειάζεται να υπολογίσει:

$$\begin{aligned} aC_0 &= kQ = (y_1, y_2), \\ c_i y_i^{-1} \pmod{p} &= m_i, \quad i = 1, 2. \end{aligned}$$

Με αυτόν τον τρόπο, ο A λαμβάνει το μήνυμα (m_1, m_2) .

Πολύ σημαντικό για την ασφάλεια του μηνύματος αποτελεί το γεγονός ότι ο ακέραιος k πρέπει να παραμείνει μυστικός. Διαφορετικά, ένας επιτιθέμενος θα ήταν σε θέση να υπολογίσει το σημείο $kQ = (y_1, y_2)$ και συνεπώς να ανακαλύψει το μήνυμα. Ο διακριτός λογάριθμος του Q ως προς τη βάση P ισούται με το ιδιωτικό κλειδί a , ενώ ο διακριτός λογάριθμος του kQ ως προς τη βάση Q αποτελεί τον ακέραιο k .

Αντιλαμβανόμαστε το πόσο σημαντικό είναι να επιλέξουμε την κατάλληλη ελλειπτική καμπύλη, έτσι ώστε το πρόβλημα να είναι υπολογιστικά αδύνατο να επιλυθεί, καθώς η ασφάλεια του κρυπτοσυστήματος βασίζεται στη δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου πάνω στην ελλειπτική καμπύλη. [20]

Παράδειγμα 3.2 Ο χρήστης A επιλέγει έναν πρώτο αριθμό $p = 13$, την ελλειπτική καμπύλη E , η οποία περιγράφεται από την εξίσωση $y^2 = x^3 + 4x + 4$ στο $\mathbb{F}_{13}$ και το σημείο $P = (1, 3) \in E(\mathbb{F}_{13})$.

Ο χρήστης A διαλέγει το ιδιωτικό κλειδί $a = 2$ και υπολογίζει

$$Q = aP = 2(1, 3) = (12, 8).$$

Το δημόσιο κλειδί είναι $(13, E, P, Q)$.

Ο χρήστης B επιθυμεί να στείλει το μήνυμα

$$m = (12, 7).$$

Επιλέγει ως ιδιωτικό κλειδί το $k = 5$ και με τη βοήθεια του δημόσιου κλειδιού του A υπολογίζει:

$$(y_1, y_2) = kQ = 5(12, 8) = (10, 11),$$

$$C_0 = kP = 5(1, 3) = (10, 2),$$

$$c_1 \equiv y_1 m_1 \bmod 13 \equiv 10 \cdot 12 \bmod 13 \equiv 3 \bmod 13,$$

$$c_2 \equiv y_2 m_2 \bmod 13 \equiv 11 \cdot 7 \bmod 13 \equiv 12 \bmod 13$$

και στέλνει στον A το κρυπτογραφημένο μήνυμα

$$C = (C_0, c_1, c_2) = ((10, 2), 3, 12).$$

Τέλος, για την αποκρυπτογράφηση, ο A υπολογίζει

$$aC_0 = 2(10, 2) = (10, 11) = (y_1, y_2),$$

$$m_1 \equiv c_1 y_1^{-1} \bmod 13 \equiv 3 \cdot 10^{-1} \bmod 13 \equiv 3 \cdot 4 \bmod 13 \equiv 12 \bmod 13$$

$$m_2 \equiv c_2 y_2^{-1} \bmod 13 \equiv 12 \cdot 11^{-1} \bmod 13 \equiv 12 \cdot 6 \bmod 13 \equiv 7 \bmod 13$$

και λαμβάνει το μήνυμα

$$m = (12, 7).$$

Για περισσότερες πληροφορίες, ο αναγνώστης μπορεί να ανατρέξει στο [20].

3.6 Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης

Ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης ECDSA (Elliptic Curve Digital Signature Algorithm) αποτελεί μία παραλλαγή του αλγορίθμου ψηφιακής υπογραφής DSA (Digital Signature Algorithm) με τη χρήση ελλειπτικών καμπυλών.

Πριν προχωρήσουμε στην περιγραφή του αλγορίθμου ψηφιακής υπογραφής, θα ορίσουμε τη **συνάρτηση κατακερματισμού** (hash function), η οποία θα μας χρειαστεί στη συνέχεια.

Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται για τη διασφάλιση της ακεραιότητας των δεδομένων σε συνδυασμό με τα σχήματα ψηφιακών υπογραφών. Πιο συγκεκριμένα, πραγματοποιείται ο κατακερματισμός του μηνύματος και στη συνέχεια η τιμή κατακερματισμού, η οποία αντιπροσωπεύει το μήνυμα υπογράφεται αντί του αρχικού μηνύματος.

Ορισμός 3.1 Μία συνάρτηση κατακερματισμού (hash function) είναι μία συνάρτηση h , η οποία έχει τις εξής ιδιότητες:

- *Συμπίεση (compression)*: Η h αντιστοιχίζει μια είσοδο x τυχαίου πεπερασμένου μήκους $bits$ σε μια έξοδο με σταθερό μήκος $n bits$.
- *Ευκολία υπολογισμού*: Δεδομένης της h συνάρτησης και μιας εισόδου x , η τιμή $h(x)$ είναι εύκολο να υπολογιστεί.

Έστω η συνάρτηση κατακερματισμού h , με εισόδους x, x' και εξόδους y, y' . Τότε ισχύουν οι παρακάτω ιδιότητες:

1. *Αντίσταση στην προεικόνα (Preimage resistance)*: Είναι αδύνατο να βρεθεί μια προεικόνα x' , έτσι ώστε

$$h(x') = y$$

όταν δίνεται μια τιμή y για την οποία δεν είναι γνωστή κάποια αντίστοιχη είσοδος. Δηλαδή, για όλες τις εξόδους είναι αδύνατο υπολογιστικά να βρεθεί κάποια είσοδος που να παράγει αυτήν την έξοδο.

2. *Αντίσταση στη δεύτερη προεικόνα (Second - Preimage resistance):* Έστω x μία είσοδος. Τότε δε μπορεί να βρεθεί μία διαφορετική είσοδος $x' \neq x$, έτσι ώστε να ισχύει η σχέση

$$h(x) = h(x').$$

3. *Αντίσταση σε συγκρούσεις (Collision Resistance):* Είναι υπολογιστικά αδύνατο να βρεθούν δύο διαφορετικοί είσοδοι x, x' έτσι ώστε να έχουν την ίδια έξοδο κατακερματισμού. Δηλαδή δε μπορεί να ισχύει η ιδιότητα

$$h(x) = h(x').$$

(Στην περίπτωση αυτή, η επιλογή των εισόδων x, x' είναι ελεύθερη).
[18]

Επιστρέφουμε στον αλγόριθμο ψηφιακής υπογραφής.

Ο χρήστης A επιλέγει μία ελλειπτική καμπύλη E πάνω στο σώμα $\mathbb{F}_p$, ένα σημείο $P \in E(\mathbb{F}_p)$, με τάξη έναν πρώτο αριθμό q και μέγεθος τουλάχιστον 160 bits.

Δημιουργία Κλειδιών

Ο χρήστης A επιλέγει τυχαία έναν αριθμό $a \in \{1, \dots, q-1\}$ και υπολογίζει $Q = aP$. Στη συνέχεια, δημοσιεύει τη συνάρτηση κατακερματισμού

$$h: \{0, 1\}^* \rightarrow \{0, \dots, q-1\}.$$

Η πεντάδα (p, q, E, P, Q) αποτελεί το δημόσιο κλειδί του χρήστη A , ενώ ο αριθμός a είναι το ιδιωτικό του κλειδί.

Δημιουργία Υπογραφής

Έστω ότι ο χρήστης A επιθυμεί να υπογράψει το μήνυμα $m \in \{0, 1\}^*$. Τότε χρειάζεται να ακολουθήσει τα εξής βήματα:

1. Επιλογή τυχαίου ακέραιου αριθμού k στο σύνολο $\{2, \dots, q-1\}$.
2. Υπολογισμός του σημείου $kP = (x_1, y_1)$ και $r = x_1 \bmod q$. Αν $r = 0$, τότε επιλέγεται καινούργιο k και η διαδικασία επαναλαμβάνεται.
3. Υπολογισμός του $k^{-1} \bmod q$ και $h(m)$.

4. Υπολογισμός του $s = k^{-1} (h(m) + ar) \bmod q$. Αν $s = 0$, τότε τα παραπάνω βήματα εκτελούνται ξανά.

Η υπογραφή είναι το ζεύγος (r, s) .

Επαλήθευση Υπογραφής

Ο χρήστης Β για να επαληθεύσει το μήνυμα ακολουθεί τα βήματα:

1. Έλεγχος ότι $r, s \in \{1, \dots, q - 1\}$.
2. Υπολογισμός του $w = s^{-1} \bmod q$ και $h(m)$.
3. Υπολογισμός του $u_1 = wh(m) \bmod q$.
4. Υπολογισμός του $u_2 = wr \bmod q$.
5. Υπολογισμός του σημείου $u_1 P + u_2 Q = (x_0, y_0)$.
6. Η υπογραφή είναι έγκυρη αν $r = x_0 \bmod q$.

Αν το μήνυμα έχει υπογραφεί σωστά, τότε η εξίσωση επαλήθευσης ισχύει. Πράγματι,

$$(x_0, y_0) = u_1 P + u_2 Q = wh(m)P + wr(aP) = w(h(m) + ar)P$$

και

$$s = k^{-1}(h(m) + ar) \bmod q.$$

Επομένως, $k = w(h(m) + ar) \bmod q$.

Αντικαθιστώντας στην παραπάνω σχέση, προκύπτει ότι

$$(x_0, y_0) = kP.$$

Αυτό σημαίνει ότι, η τετμημένη x_0 του σημείου kP ικανοποιεί τη σχέση $u = r$, οπότε η υπογραφή είναι έγκυρη.

Η ασφάλεια του ιδιωτικού κλειδιού a βασίζεται στη δυσκολία υπολογισμού του διακριτού λογαρίθμου του Q ως προς P . Επίσης, ο ακέραιος k πρέπει να παραμένει μυστικός και να αλλάζει κάθε φορά που υπογράφεται ένα μήνυμα.
[20]

Κεφάλαιο 4

Pairing - Based Cryptography

Το κεφάλαιο αυτό αφορά τις ζεύξεις (pairings), οι οποίες αποτελούν ένα ιδιαίτερα σημαντικό κρυπτογραφικό εργαλείο, καθώς αξιοποιούνται σε ένα ευρύ φάσμα εφαρμογών.

4.1 Εισαγωγή στα Pairing

Μια ζεύξη είναι μία συνάρτηση η οποία αντιστοιχεί στοιχεία από μία ομάδα πηγή G_1 σε μία ομάδα προορισμό G_T . Αυτό έχει ως αποτέλεσμα, την διευκόλυνση επίλυσης προβλημάτων, τα οποία στο G είναι δύσκολα, αλλά μέσω της ζεύξης στο G_T μπορούν να γίνουν εύκολα. [2]

4.2 Διγραμμικές Ζεύξεις

Έστω μία προσθετική ομάδα $G_1 = \langle P \rangle$, τάξης n , όπου n πρώτος και με ουδέτερο στοιχείο το ∞ . Επίσης, έστω η πολλαπλασιαστική ομάδα G_T , τάξης n με ουδέτερο στοιχείο το 1.

Ορισμός 4.1 Μία διγραμμική ζεύξη (Bilinear Pairing) στο (G_1, G_T) είναι μία απεικόνιση

$$\hat{e} : G_1 \times G_1 \rightarrow G_T,$$

η οποία ικανοποιεί τις ακόλουθες ιδιότητες:

1. *Διγραμμικότητα (Bilinearity)*: Για κάθε $R, S, T \in G_1$ ισχύει

$$\hat{e}(R + S, T) = \hat{e}(R, T) \hat{e}(S, T),$$

$$\hat{e}(R, S + T) = \hat{e}(R, S) \hat{e}(R, T).$$

2. Μη - εκφυλισμένη (Non - Degeneracy):

$$\hat{e}(P, P) \neq 1.$$

3. Υπολογισιμότητα (Computability): Η τιμή της ζεύξης $\hat{e}$ μπορεί να υπολογιστεί αποδοτικά.

Επίσης, για τις διγραμμικές ζεύξεις ισχύουν οι ιδιότητες:

$$1. \hat{e}(S, \infty) = 1 \text{ και } \hat{e}(\infty, S) = 1.$$

$$2. \hat{e}(S, -T) = \hat{e}(-S, T) = \hat{e}(S, T)^{-1}.$$

$$3. \hat{e}(aS, bT) = \hat{e}(S, T)^{ab}, \text{ για κάθε } a, b \in \mathbb{Z}.$$

$$4. \hat{e}(S, T) = \hat{e}(T, S).$$

$$5. \text{ Αν } \hat{e}(S, R) = 1, \text{ για κάθε } R \in G_1, \text{ τότε } S = \infty.$$

Το πρόβλημα του διακριτού λογαρίθμου DLP (Discrete Logarithm Problem) στο G_1 μπορεί να αναχθεί στο G_T με τη βοήθεια των ζεύξεων.

Πράγματι, αν επιθυμούμε να υπολογίσουμε το διακριτό λογάριθμο (P, Q) στο G_1 , όπου $Q = xP$, τότε

$$\hat{e}(P, Q) = \hat{e}(P, xP) = \hat{e}(P, P)^x.$$

Συνεπώς,

$$\log_P Q = \log_g h,$$

όπου τα $g = \hat{e}(P, P)$ και $h = \hat{e}(P, Q)$ αποτελούν στοιχεία του G_T .

Η ασφάλεια αρκετών πρωτοκόλλων που βασίζονται σε ζεύγη εξαρτάται από την δυσκολία επίλυσης του Διγραμμικού Προβλήματος των Diffie - Hellman (BDHP).

Ορισμός 4.2 Έστω $\hat{e}$ η διγραμμική ζεύξη στο (G_1, G_T) . Το πρόβλημα του Διγραμμικού Προβλήματος των Diffie - Hellman (BDHP) είναι το εξής:

Δίνονται τα σημεία P, aP, bP, cP . Ζητείται να υπολογιστεί

$$\hat{e}(P, P)^{abc}.$$

Η δυσκολία του Διγραμμικού Προβλήματος των Diffie - Hellman συνεπάγεται τη δυσκολία του Προβλήματος των Diffie - Hellman (DHP) τόσο στο G_1 , όσο και στο G_T . Αν ήταν δυνατόν να λυθεί το DHP στο G_1 , τότε θα μπορούσε να λυθεί και το BDHP υπολογίζοντας το abP και στη συνέχεια

$$\hat{e}(abP, cP) = \hat{e}(P, P)^{abc}.$$

Επίσης, αν το DHP στο G_T μπορούσε να λυθεί, τότε θα ήταν δυνατόν να λυθεί και το BDHP υπολογίζοντας

$$g = \hat{e}(P, P),$$

$$g^{ab} = \hat{e}(aP, bP),$$

$$g^c = \hat{e}(P, cP)$$

και στη συνέχεια αρκεί να υπολογιστεί το g^{abc} . Δε γνωρίζουμε κάτι περαιτέρω για τη δυσκολία του προβλήματος BDHP. Όμως, θεωρείται ότι είναι τόσο δύσκολο, όσο το πρόβλημα DHP στο G_1 , και στο G_T .

Για περισσότερες πληροφορίες, ο αναγνώστης παραπέμπεται να ανατρέξει στα [2],[17],[23].

4.3 Σημεία Στρέψης

Ως σημεία στρέψης (torsion points) ορίζουμε τα σημεία εκείνα που έχουν πεπερασμένη τάξη. Ο ρόλος τους στη μελέτη ελλειπτικών καμπυλών είναι σπουδαίος και για αυτό το λόγο αξίζει να μελετηθούν. Η ομάδα των σημείων

μίας ελλειπτικής καμπύλης επί ενός πεπερασμένου σώματος είναι πεπερασμένη και επομένως όλα τα σημεία της είναι σημεία στρέψης.

Έστω μια ελλειπτική καμπύλη E ορισμένη στο σώμα K και n ένας θετικός ακέραιος. Τότε

$$E[n] = \{P \in E(\bar{K}) \mid nP = \infty\},$$

όπου με $\bar{K}$ συμβολίζουμε το αλγεβρικό κάλυμμα του K . Συνεπώς, το $E[n]$ περιέχει σημεία με συντεταγμένες στο $\bar{K}$, όχι μόνο στο K .

Θεώρημα 4.1 Έστω E μια ελλειπτική καμπύλη ορισμένη πάνω στο σώμα K και n ένας θετικός ακέραιος. Αν η χαρακτηριστική του K δεν διαιρεί το n ή ισούται με 0, τότε

$$E[n] = \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Αν η χαρακτηριστική του K ισούται με $p > 0$ και $p \mid n$, γράφουμε $n = p^r n'$, με $p \nmid n'$. Τότε

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n \quad \text{ή} \quad \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Για την απόδειξη του παραπάνω θεωρήματος ο αναγνώστης παραπέμπεται στο [28].

4.4 Διαιρέτες

Στο κεφάλαιο αυτό παρουσιάζονται κάποιες θεμελιώδεις έννοιες της αλγεβρικής γεωμετρίας, οι οποίες κρίνονται απαραίτητες για τη βέλτιστη κατανόηση των υπολογισμών κρυπτογραφικών ζεύξεων.

Ας είναι E μία ελλειπτική καμπύλη η οποία ορίζεται υπεράνω ενός αλγεβρικά κλειστού σώματος K από μία εξίσωση του Weierstrass $F(x,y) = 0$. Καλούμε *διαιρέτη* D της E κάθε τυπικό άθροισμα της μορφής:

$$D = \sum_{P \in \mathcal{E}(\overline{\mathbb{F}}_q)} n_P(P), \quad \text{όπου } n_P \in \mathbb{Z}.$$

Το σύνολο όλων των διαιρετών στην $\mathcal{E}$ συμβολίζεται με $\text{Div}_{\overline{\mathbb{F}}_q}(\mathcal{E})$.

Το σύνολο αυτό συγκροτεί ομάδα, όπου η πρόσθεση των διαιρετών ορίζεται κανονικά και το ουδέτερο στοιχείο είναι ο διαιρέτης, με $n_P = 0$, για κάθε P .

Ο βαθμός του διαιρέτη D ορίζεται ως εξής:

$$\text{Deg}(D) = \sum_{P \in \mathcal{E}(\overline{\mathbb{F}}_q)} n_P.$$

Θεωρούμε τον δακτύλιο πηλίκο $K[\mathcal{E}] = K[x,y]/(F)$ ο οποίος είναι ακέραια περιοχή, καθώς το πολυώνυμο $F(x,y)$ είναι ανάγωγο. Το σώμα κλασμάτων $K(\mathcal{E})$ του $K[\mathcal{E}]$ καλείται *σώμα συναρτήσεων* της ελλειπτικής καμπύλης $\mathcal{E}$.

Ας είναι f μία συνάρτηση του $K(\mathcal{E})$ και P ένα σημείο της $\mathcal{E}$. Λέμε ότι η f είναι *ορισμένη* στο P , αν υπάρχει ένα ρητό κλάσμα $G(x,y)/H(x,y)$ το οποίο αναπαριστά την f και ισχύει $f(P) = G(P)/H(P) \in K$. Το σύνολο όλων των συναρτήσεων οι οποίες ορίζονται σ' ένα σημείο P αποτελεί ένα τοπικό υποδακτύλιο του $K(\mathcal{E})$ ο οποίος συμβολίζεται με $\mathcal{O}_P(\mathcal{E})$.

Ορισμός 4.3 Ο δακτύλιος $\mathcal{O}_P(\mathcal{E})$ καλείται *τοπικός δακτύλιος* της ελλειπτικής καμπύλης $\mathcal{E}$ στο P .

Ας είναι R μία ακέραια περιοχή και L το σώμα κλασμάτων της. Λέμε ότι ο R είναι *δακτύλιος διακριτής εκτίμησης*, αν είναι ένας δακτύλιος κύριων ιδεωδών ο οποίος έχει ένα μοναδικό πρώτο ιδεώδες $\mathfrak{p} \neq \{0\}$. Ας είναι t ένας γεννήτορας του $\mathfrak{p}$. Τότε, κάθε $z \in L \setminus \{0\}$ γράφεται με μοναδικό τρόπο στη μορφή

$$z = t^n u,$$

όπου n είναι ακέραιος ≥ 0 και u αντιστρέψιμο στοιχείο του A . Ο εκθέτης n καλείται *τάξη* του z και συμβολίζεται με $\text{ord}_R(z)$ ή πιο απλά με $\text{ord}(z)$. Επίσης, θέτουμε $\text{ord}(0) = \infty$. Έτσι, έχουμε

$$R = \{z \in L / \text{ord}(z) \geq 0\}$$

και

$$\mathfrak{p} = \{z \in L / \text{ord}(z) > 0\}.$$

Αν $\text{ord}_R(z) > 0$, τότε λέμε ότι το z μηδενίζεται στο R , και αν $\text{ord}_R(z) < 0$, ότι έχει ένα πόλο στο R .

Πρόταση 4.1 [3] Ο τοπικός δακτύλιος της ελλειπτικής καμπύλης E στο σημείο P , $\mathcal{O}_P(E)$, είναι ένας δακτύλιος διακριτής εκτίμησης.

Ας είναι $f \in K(E)$. Συμβολίζουμε με $\text{ord}_P(f)$ την τάξη του f η οποία ορίζεται από τον δακτύλιο $\mathcal{O}_P(E)$. Ο *διαιρέτης* (f) της f ορίζεται ως

$$(f) = \sum_{P \in E(\overline{\mathbb{F}}_q)} \text{ord}_P(f)(P).$$

4.5 Weil Pairings

Το 1940, ο Andre Weil εισήγαγε το ζεύγος Weil (Weil Pairing), το οποίο συμβάλλει σημαντικά στη θεωρητική μελέτη της αριθμητικής των ελλειπτικών καμπυλών και των Αβελιανών πολλαπλοτήτων. Η χρησιμότητα του ζεύγους Weil σε κρυπτογραφικές κατασκευές έχει καταστήσει τη μελέτη του ιδιαίτερα σημαντική, καθώς αποτελεί βασικό εργαλείο για την ανάπτυξη προηγμένων κρυπτογραφικών πρωτοκόλλων.

Έστω η ελλειπτική καμπύλη

$$E: y^2 = x^3 + Ax + B$$

πάνω στο σώμα K και n ένας ακέραιος που δεν διαιρείται από την χαρακτηριστική του K . Τότε $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Η ομάδα των n -οστών ριζών της μονάδας στο $\overline{K}$ είναι το σύνολο

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}.$$

Επίσης, η εξίσωση $x^n = 1$ δεν έχει πολλαπλές ρίζες, καθώς η χαρακτηριστική του K δεν διαιρεί το n . Επομένως, έχει n ρίζες στο $\overline{K}$ και η μ_n αποτελεί μία κυκλική ομάδα τάξης n .

Ορίζουμε ως πρωταρχική n -οστή ρίζα της μονάδας, κάθε γεννήτορα ζ της μ_n . Ισοδύναμα $\zeta^k = 1$ αν και μόνο αν το n διαιρεί το k .

Θεώρημα 4.2 Έστω $\mathcal{E}$ μία ελλειπτική καμπύλη ορισμένη πάνω στο σώμα K και n ένας θετικός ακέραιος. Υποθέτουμε ότι η χαρακτηριστική του K δεν διαιρεί το n . Τότε υπάρχει μία ζεύξη

$$e_n : \mathcal{E}[n] \times \mathcal{E}[n] \rightarrow \mu_n,$$

η οποία ονομάζεται Weil pairing και ικανοποιεί τις παρακάτω ιδιότητες:

1. Το e_n είναι διγραμμικό ως προς κάθε μεταβλητή. Δηλαδή,

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

και

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2),$$

για κάθε $S, S_1, S_2, T, T_1, T_2 \in \mathcal{E}[n]$.

2. Το e_n είναι μη εκφυλισμένο ως προς κάθε μεταβλητή. Αυτό σημαίνει ότι, αν $e_n(S, T) = 1$, για κάθε $T \in \mathcal{E}[n]$, τότε $S = \infty$. Επίσης, αν $e_n(S, T) = 1$, για κάθε $S \in \mathcal{E}[n]$, τότε $T = \infty$.

3. $e_n(T, T) = 1$, για κάθε $T \in \mathcal{E}[n]$.

4. $e_n(T, S) = e_n(S, T)^{-1}$, για κάθε $S, T \in \mathcal{E}[n]$.

5. $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$, για κάθε αυτομορφισμό σ του $\bar{K}$, έτσι ώστε το σ να αποτελεί την ταυτοτική απεικόνιση των συντελεστών της $\mathcal{E}$.

6. Ισχύει $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$, για κάθε διαχωρίσιμο ενδομορφισμό α της $\mathcal{E}$. Αν οι συντελεστές της $\mathcal{E}$ ανήκουν στο πεπερασμένο σώμα $\mathbb{F}_q$, τότε η σχέση αυτή ισχύει και όταν το α είναι ο ενδομορφισμός Frobenius φ_q .

Για την απόδειξη του θεωρήματος, ανατρέξτε στο [28].

Ορισμός 4.4 Ένας διαιρέτης $D \in \text{Div}(\mathcal{E})$ λέγεται κύριος (principal), αν $D = \text{div}(f)$, για κάποια συνάρτηση $f \in \overline{K}(\mathcal{E})$. Δύο διαιρέτες λέγονται γραμμικά ισοδύναμοι, και γράφουμε $D_1 \sim D_2$, αν ο διαιρέτης $D_1 - D_2$ είναι κύριος. [23]

Ορισμός 4.5 Το ζευγάρισμα του Weil σε πεπερασμένα σώματα

Έστω $P, Q \in \mathcal{E}(\mathbb{F}_{q^k})[r]$ και ας είναι D_P και D_Q μηδενικού βαθμού διαιρέτες, με

$$D_P \sim (P) - (O) \quad \text{και} \quad D_Q \sim (Q) - (O).$$

Υπάρχουν συναρτήσεις f, g έτσι ώστε

$$(f) = rD_P \quad \text{και} \quad (g) = rD_Q.$$

Το ζευγάρισμα του Weil w_r είναι η απεικόνιση:

$$w_r : \mathcal{E}(\mathbb{F}_{q^k})[r] \times \mathcal{E}(\mathbb{F}_{q^k})[r] \rightarrow \mu_r$$

η οποία ορίζεται ως

$$w_r(P, Q) = \frac{f(D_Q)}{g(D_P)}. [10]$$

4.6 Tate - Lichtenbaum Pairing

Το ζευγάρισμα του Weil χρησιμοποιείται για τον ορισμό άλλων ζεύξεων στις ελλειπτικές καμπύλες. Στην παράγραφο αυτή, αναλύεται η ζεύξη Tate - Lichtenbaum, η οποία έχει τόσο θεωρητικές, όσο και κρυπτογραφικές εφαρμογές.

Θεώρημα 4.3 Έστω $\mathcal{E}$ μια ελλειπτική καμπύλη ορισμένη πάνω στο πεπερασμένο σώμα $\mathbb{F}_q$ και n ένας ακέραιος, τέτοιος ώστε $n \mid q - 1$. Το $\mathcal{E}(\mathbb{F}_{q^k})[n]$ αντιπροσωπεύει τα στοιχεία του $\mathcal{E}(\mathbb{F}_q)$ των οποίων η τάξη διαιρεί το n και ας είναι

$$\mu_n = \{x \in \mathbb{F}_q \mid x^n = 1\}.$$

Έστω $P \in \mathcal{E}(\mathbb{F}_q)[n]$ και $Q \in \mathcal{E}(\mathbb{F}_q)$ και επιλέγουμε $R \in \mathcal{E}(\overline{\mathbb{F}_q})$ έτσι ώστε $nR = Q$. Συμβολίζουμε με e_n τη ζεύξη Weil τάξης n , και με $\varphi = \varphi_q$ τον ενδομορφισμό Frobenius q -οστής δύναμης. Ορίζουμε

$$\tau_n(P, Q) = e_n(P, R - \varphi(R)).$$

Τότε, η

$$\tau_n: \mathcal{E}(\mathbb{F}_q)[n] \times \mathcal{E}(\mathbb{F}_q)/n\mathcal{E}(\mathbb{F}_q) \rightarrow \mu_n$$

είναι μία καλά ορισμένη, μη εκφυλισμένη διγραμμική ζεύξη.

Η παραπάνω ζεύξη καλείται τροποποιημένη ζεύξη Tate - Lichtenbaum. Για την αρχική ζεύξη αρκεί να λάβουμε τη n -οστή ρίζα της τ_n και έτσι προκύπτει η ζεύξη

$$\langle \cdot, \cdot \rangle_n: \mathcal{E}(\mathbb{F}_q)[n] \times \mathcal{E}(\mathbb{F}_q)/n\mathcal{E}(\mathbb{F}_q) \rightarrow \mathbb{F}_q^x / (\mathbb{F}_q^x)^n. \quad [28]$$

4.7 Πρωτόκολλα

Στην παράγραφο αυτή, παρουσιάζονται τρία πρωτόκολλα που βασίζονται στις ζεύξεις.

4.7.1 Τριμερής Ανταλλαγή Κλειδιού

Η ανταλλαγή κλειδιών Diffie - Hellman μεταξύ τριών ατόμων υπήρξε από τις πρώτες εφαρμογές ζεύξεων στην κρυπτογραφία και προτάθηκε από τον Joux. Όπως τροποποιήθηκε από τον Verheul πρόκειται για μία διγραμμική ζεύξη στις ομάδες (G_1, G_T) για την οποία το Διγραμμικό Πρόβλημα Diffie - Hellman (BDHP) θεωρείται υπολογιστικά ανεπίλυτο.

Αρχικά, ο χρήστης A επιλέγει έναν τυχαίο μυστικό ακέραιο $a \in [1, n - 1]$ και στη συνέχεια δημοσιεύει το σημείο aP στους άλλους δύο χρήστες.

Με τον ίδιο τρόπο, οι χρήστες B, C διαλέγουν αντιστοίχως και εκείνοι από έναν τυχαίο ακέραιο $b, c \in [1, n - 1]$ και δημοσιεύουν τα σημεία bP και cP .

Δεδομένου ότι ο χρήστης A έχει λάβει τα σημεία bP και cP (όπως και οι χρήστες B,C) είναι πλέον σε θέση να υπολογίσει το κοινό μυστικό κλειδί

$$K = \hat{e}(bP, cP)^a = \hat{e}(P, P)^{abc}.$$

Αν κάποιος επιθυμεί να υπολογίσει το μυστικό κλειδί K έρχεται αντιμέτωπος με την επίλυση του Διγραμμικού Προβλήματος Diffie - Hellman (BDHP). [17]

4.7.2 Σύντομες Υπογραφές

Τα περισσότερα σχήματα ψηφιακών υπογραφών που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου, όπως το DSA προέρχονται από το σχήμα υπογραφής ElGamal. Σε αυτά τα σχήματα, οι υπογραφές αποτελούνται από ένα ζεύγος ακεραίων *modulo* n , όπου n είναι η τάξη της ομάδας $G_1 = \langle P \rangle$. Το πρώτο σχήμα σύντομης υπογραφής (Short Signature) προτάθηκε από τους Boneh, Lynn και Shacham (BLS), κατά το οποίο η υπογραφή αποτελείται από ένα μόνο στοιχείο ομάδας, το οποίο μπορεί να περιγραφεί με περίπου τον ίδιο αριθμό *bits* που χρειάζεται για την αναπαράσταση ενός ακεραίου *modulo* n .

Το σχήμα σύντομης υπογραφής BLS βασίζεται σε μία διγραμμική ζεύξη $\hat{e}$ μεταξύ των ομάδων (G_1, G_T) , για την οποία το πρόβλημα Diffie - Hellman στην ομάδα G_1 είναι αρκετά δύσκολο. Επιπλέον, χρησιμοποιεί συνάρτηση κατακερματισμού

$$H : \{0, 1\}^* \rightarrow G_1 \setminus \{\infty\}.$$

Ο χρήστης A επιλέγει ως ιδιωτικό κλειδί έναν τυχαίο ακέραιο $a \in [1, n - 1]$ και στη συνέχεια υπολογίζει το δημόσιο κλειδί του

$$A = aP.$$

Έπειτα, για να υπογράψει ένα μήνυμα $m \in \{0, 1\}^*$ παράγει τον κατακερματισμό $M = H(m)$ και στη συνέχεια δημιουργεί την υπογραφή

$$S = aM.$$

Για την επαλήθευση της υπογραφής, αν κάποιος γνωρίζει το δημόσιο κλειδί του χρήστη A, αρκεί να υπολογίσει το

$$M = H(m)$$

και να ελέγξει αν η τετράδα (P, A, M, S) ικανοποιεί το DDHP (Decisional Diffie-Hellman Problem) στο G_1 . Πιο συγκεκριμένα, αρκεί να ελέγξει αν ισχύει:

$$\hat{e}(P, S) = \hat{e}(A, M).$$

Η πλαστογράφηση της υπογραφής του χρήστη A σε ένα μήνυμα m είναι υπολογιστικά δυσεπίλυτη, καθώς χρειάζεται να υπολογίσει την ποσότητα

$$S = aM,$$

έχοντας γνώση μόνο των P, A και $M = H(m)$. Το πρόβλημα αυτό συνιστά περίπτωση του προβλήματος Diffie-Hellman στο G_1 . [2] , [17]

4.7.3 Κρυπτογράφηση με βάση την Ταυτότητα

Το 1984, ο Shamir εισήγαγε την *κρυπτογραφία βασισμένη στην ταυτότητα* (Identity - Based Encryption), κατά την οποία το δημόσιο κλειδί ενός χρήστη προκύπτει από κάποιο στοιχείο ταυτοποίησης του, όπως η διεύθυνση του ηλεκτρονικού του ταχυδρομείου. Πιο αναλυτικά, θεωρούμε ότι όλοι οι χρήστες διαθέτουν μία ταυτότητα και υπάρχει μία έμπιστη πηγή, η οποία αναλαμβάνει τη δημιουργία του ιδιωτικού κλειδιού χρησιμοποιώντας την ταυτότητα και παραδίδοντας το στο χρήστη. Μέσω της ταυτότητας του παραλήπτη και του δημόσιου κλειδιού της έμπιστης πηγής, κάθε χρήστης έχει την ευκαιρία να κρυπτογραφήσει ένα μήνυμα.

Οι Boneh και Franklin κατόρθωσαν την υλοποίηση του με τη βοήθεια των ζεύξεων. Αναλυτικότερα, το σχήμα αυτό στηρίζεται στην ύπαρξη διγραμμικής ζεύξης e μεταξύ των ομάδων (G_1, G_T) , όπου το BDDH (Bilinear Decisional Diffie - Hellman Problem) παρουσιάζει σημαντικές δυσκολίες. Επίσης, χρησιμοποιεί τις συναρτήσεις κατακερματισμού

$$H_1 : \{0, 1\}^* \rightarrow G_1 \setminus \{\infty\},$$

$$H_2 : G_T \rightarrow \{0, 1\}^l,$$

όπου l είναι το μήκος του μηνύματος σε *bits*.

- Η έμπιστη πηγή έχει ως ιδιωτικό κλειδί έναν τυχαίο ακέραιο $t \in [1, \dots, n - 1]$ και ως δημόσιο κλειδί $T = tP$. Όλοι οι χρήστες έχουν πρόσβαση στο δημόσιο κλειδί T .
- Για την παραγωγή του ιδιωτικού κλειδιού d_A του χρήστη A , η έμπιστη πηγή δημιουργεί την ταυτότητα του χρήστη A (ID_A) και υπολογίζει

$$d_A = tH_1(ID_A).$$

Έπειτα, το ιδιωτικό κλειδί d_A στέλνεται στο χρήστη A με ασφάλεια.

- Για την κρυπτογράφηση ενός μηνύματος $m \in \{0, 1\}^l$ προς τον χρήστη A , ο χρήστης B υπολογίζει

$$Q_A = H_1(ID_A),$$

επιλέγει έναν τυχαίο ακέραιο $r \in [1, n - 1]$ και υπολογίζει

$$R = rP,$$

$$c = m \oplus H_2(\hat{e}(Q_A, T)^r),$$

όπου το σύμβολο $\oplus$ εκφράζει τη λογική πράξη XOR.

Το κρυπτοκείμενο είναι το ζεύγος (R, c) , το οποίο στέλνεται στον χρήστη A .

- Για την αποκρυπτογράφηση του μηνύματος, ο χρήστης A χρησιμοποιεί το ιδιωτικό κλειδί d_A και υπολογίζει:

$$m = c \oplus H_2(\hat{e}(d_A, R)).$$

Η αποκρυπτογράφηση είναι σωστή, διότι ισχύει:

$$\hat{e}(d_A, R) = \hat{e}(tQ_A, rP) = \hat{e}(Q_A, tP)^r = \hat{e}(Q_A, T)^r.$$

Η ασφάλεια του κρυπτοσυστήματος απορρέει από τη δυσκολία το Διγραμμικού Προβλήματος Diffie - Hellman (BDH). [2], [17]

Βιβλιογραφία:

- [1] Γιάννης Αντωνιάδης και Αριστείδης Κοντογεώργης, Πεπερασμένα σώματα & Κρυπτογραφία , Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα, 2015.
- [2] Ευστάθιος Ζάχος, Αριστείδης Παγουρτζής και Παναγιώτης Γρόντας, Υπολογιστική Κρυπτογραφία, Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2015.
- [3] Δημήτριος Πουλάκης, Αλγεβρική Γεωμετρία, Εκδόσεις Ζήτη, 2018.
- [4] Δημήτριος Πουλάκης, Εισαγωγή στη Γεωμετρία των Αλγεβρικών Καμπυλών, Εκδόσεις Ζήτη, 2006.
- [5] Δημήτριος Πουλάκης, Κρυπτογραφία, Εκδόσεις Ζήτη, 2004.
- [6] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and Christiane Peters, Twisted Edwards Curves, International Conference in Cryptology in Africa, 2008.
- [7] W. Castryck, S. Galbraith and R. Farashahi, Efficient arithmetic on elliptic curves using a mixed Edwards - Montgomery representation, IACR Cryptology ePrint Archive, 2008.
- [8] J.S Chahal, Topics in Number Theory, The University Series in Mathematics, 1988.
- [9] J.S Chahal and B. Osseman, The Riemann Hypothesis for Elliptic Curves, The American Mathematical Monthly, Vol. 115, No.5, 2008.
- [10] C. Costello, Pairings for beginners, 2012.
- [11] C. Costello and B. Smith, Montgomery curves and their arithmetic. The case of large characteristic elds, Journal of Cryptographic Engineering, 2017.
- [12] M.R.Dam, Edwards Elliptic Curves, University of Groningen, 2012.
- [13] Y. E. Housni, Edwards curves, HAL Open Science, 2018.
- [14] M. Joye and J. Quisquater, Hessian Elliptic Curves and Side-Channel Attacks, Published in C .K. Koc, D. Naccache, and C. Paar, Eds., Cryptographic Hardware and Embedded Systems - CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 402-410, Springer-Verlag, 2001.
- [15] A. H. Koblitz, N. Koblitz, A. Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift, Journal of Number Theory 131 (2011) 781-814.
- [16] N. Koblitz, A. Menezes and S. Vanstone, The State of Elliptic Curve Cryptography, 2000 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

- [17] A. Menezes, An Intoduction to Pairing-Based Cryptography, Recent Trends in Cryptography, edited by I. Luengo, volume 477 of Contemporary Mathematics, AMS-RSME, 2009, 47-65.
- [18] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
- [19] L.D.V van Nifterik, Edwards curves, Leiden University, 2023.
- [20] Dimitrios Poulakis, Mathematical Cryptology, De Gruyter, 2026.
- [21] R. Rahman. Elliptic Curves, The Group Law, and the J invariant, University of Chicago, 2016.
- [22] T. Severns, An Exposition of Elliptic Curve Cryptography, Electronic Theses, Projects, and Dissertations, California State University, San Bernardino, 2022.
- [23] J.Silverman, The Arithmetic of Elliptic Curves, Springer, 2009.
- [24] J. H. Silverman, An Intoduction to the Theory of Elliptic Curves, Brown University and NTRU Cryptosystems, Inc, 2006.
- [25] N.P.Smart, The Hessian Form of an Elliptic Curve, International Workshop on Cryptographic Hardware and Embedded Systems, 2001.
- [26] M. Soeten, Hasse's Theorem on Elliptic Curves, M.S thesis, Dept. of Mathematics, University of Groningen , 2013.
- [27] F. Stefan, An elementary proof of the group law for elliptic curves. The Group Law in Elliptic Curves, 1998.
- [28] L. C. Washington, Elliptic Curves Number Theory and Cryptography, 2nd.ed, University of Maryland, U.S.A, 2008.

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986 η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/ δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης.