ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Στοιχεία Θεωρίας Αριθμών και Εφαρμογές στην Κρυπτογραφία 9ο εξάμηνο,

Ακαδημαϊκή περίοδος 2012-2013

Ελλειπτικές καμπύλες και κρυπτογραφία

Περιεχόμενα

1 Ελλειπτικές καμπύλες

1.1 Εισαγωγή

Πολλά συστήματα κρυπτογραφίας βασίζονται σε πράξεις πάνω σε κάποια αλγεβρική ομάδα. Μπορούμε να χρησιμοποιήσουμε μία ελλειπτική καμπύλη για να ορίσουμε μία ομάδα και έπειτα περιορίζοντας τα σημεία αυτής να ορίσουμε ένα σώμα. Θα δείξουμε αρχικά τις πράξεις που ορίζονται πάνω σε μία τέτοια ομάδα στο πεδίο των πραγματικών αριθμών και μετά στο $\mathcal{F}_p$.

1.2 Ελλειπτικές καμπύλες στο $\mathcal{R}$

Μία ελλειπτική καμπύλη στο $\mathcal{R}$ μπορεί να οριστεί ως ένα set σημείων (x,y) που ικανοποιούν μία εξίσωση ελλειπτικής καμπύλης της μορφής:

$$y^2 = x^3 + a \cdot x + b \ , \ x, y, a, b \in \mathcal{R}$$

Ανάλογα με την επιλογή των a και b έχουμε μία διαφορετική ελλειπτική καμπύλη. Για να ορίσουμε μία ομάδα από μία τέτοια ελλειπτική καμπύλη θα πρέπει το $x^3 + a \cdot x + b$ να μην έχει επαναλαμβανόμενους παράγοντες, δηλαδή να ισχύει $4 \cdot a^3 + 27 \cdot b^2 \neq 0$. Σε αυτή την περίπτωση μία τέτοια ομάδα ορίζεται απο τα σημεία που αποτελούν την ελλειπτική καμπύλη μαζί με ένα ακόμα σημείο $\mathcal{O}$ που θεωρείται το σημείο στο άπειρο.

1.2.1 Ορισμένες πράξεις σε μία ελλειπτική καμπύλη πάνω στο $\mathcal{R}$

Αντίθετο σημείο Αν για δύο σημεία $P = (x_P, y_P)$ και $Q = (x_Q, y_Q)$ ισχύει ότι $Q = (x_P, -y_P)$ τότε λέμε ότι $P = -Q$. Γεωμετρικά αυτό σημαίνει οτι το Q είναι συμμετρικό του P ως προς τον άξονα x.

Πρόσθεση δύο σημείων Θα ορίσουμε την πρόσθεση δύο σημείων σε μία ελλειπτική καμπύλη γεωμετρικά. Έστω δύο σημεία P και Q για τα οποία ισχύει ότι $P \neq -Q$. Για να υπολογίσουμε το $R = P + Q$ φέρουμε μία ευθεία που τέμνει και τα δύο σημεία. Η ευθεία αυτή θα τέμνει την καμπύλη σε ακρίβως ένα σημείο ακόμα, το $-R$. Το αντίθετο αυτού είναι το άθροισμα $P+Q = R$. Για την περίπτωση όπου $P = -Q$ ισχύει $P + (-P) = \mathcal{O}$. Επίσης ισχύει ότι $P + \mathcal{O} = P$.

Διπλασιασμός σημείου Για την πρόσθεση ενός σημείου P στον εαυτό του φέρουμε ευθεία εφαπτόμενη στο P. Αν $y_P \neq 0$ τότε αυτή θα τέμνει την καμπύλη σε ένα ακόμα σημείο, έστω $-R$. Ισχύει ότι $P + P = 2 \cdot P = R$. Στην περίπτωση που $y_p = 0$ τότε $P + P = 2 \cdot P = \mathcal{O}$.

1.3 Ελλειπτικές καμπύλες πάνω από το σώμα F_p.

Οι πράξεις πάνω σε πραγματικούς αριθμούς είναι αργές και στερούνται ακρίβειας λόγω στρογγυλοποιήσεων. Καθώς οι εφαρμογές κρυπτογραφίας απαιτούν ταχύτητα και ακρίβεια στις πράξεις προτιμούνται ελλειπτικές καμπύλες στο σώμα F_p ή F_{2^m}. Για να ορίσουμε μία ελλειπτική καμπύλη στο F_p αρκεί να διαλέξουμε $a, b \in F_p$. Όλα τα σημεία (x, y) της καμπύλης θα ικανοποιούν την εξίσωση αυτής $modulop$.

1.3.1 Ορισμένες πράξεις σε μία ελλειπτική καμπύλη πάνω στο F_p

Μία γεωμετρική προσέγγιση θα αποτύχει σε αυτή την περίπτωση λόγω του πεπερασμένου πλήθους σημείων. Για το λόγο αυτό θα χρησιμοποιήσουμε τις αντίστοιχες αλγεβρικές εξισώσεις.

Αντίθετο σημείο Αν για δύο σημεία $P = (x_P, y_P)$ και $Q = (x_Q, y_Q)$ ισχύει ότι $Q = (x_P, -y_P)$ τότε λέμε ότι $P = -Q$.

Πρόσθεση δύο σημείων Έστω δύο σημεία P και Q για τα οποία ισχύει ότι $P \neq -Q$. Έστω ο συντελέστης της ευθείας απο το P στο Q

$$s = \frac{(y_P - y_Q)}{(x_P - x_Q)} \pmod{p}$$

Για το $R = P + Q$ θα ισχύει:

$$x_R = s^2 - x_P - x_Q \pmod{p}$$
$$y_R = -y_P + s \cdot (x_P - x_R) \pmod{p}$$

Διπλασιασμός σημείου Αν $y_P \neq 0$ τότε $P+P = 2 \cdot P = R$ όπου το R υπολογίζεται από τις παρακάτω σχέσεις:

$$s = \frac{(3 \cdot x_P^2 + a)}{2 \cdot y_P} \pmod{p}$$
$$x_R = s^2 - 2 \cdot x_P \pmod{p}$$
$$y_R = -y_p + s \cdot (x_P - x_R) \pmod{p}$$

1.4 Ελλειπτικές καμπύλες πάνω από το σώμα F_{2^m}.

Τα στοχεία του σώματος F_{2^m} είναι m-bit strings για το λόγω αυτό οι υπολογιστές μπορούν να εκτελέσουν αριθμητικές πράξεις πάνω σε αυτά πολύ αποδοτικά. Οι πράξεις δε διαφέρουν από αυτές που ορίσαμε παραπάνω.

2 Το πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες (ECDLP)

Κάθε σύστημα κρυπτογραφίας βασίζεται σε ένα υπολογιστικό πρόβλημα, συνήθως δύσκολο στον υπολογισμό του απουσία κάποιας πληροφορίας, π.χ. ενός secret key. Μπορούμε να φτιάξουμε συστήματα κρυπτογραφίας που βασίζονται στη δυσκολία υπολογισμού του διακριτού λογάριθμου σε ελλειπτικές καμπύλες (ECDLP).

2.1 Βαθμωτός Πολλαπλασιασμός

Ο βαθμωτός πολλαπλασιασμός ενός σημείου P της ελλειπτικής καμπύλης πάνω στο F_p με έναν ακέραιο k μικρότερο της τάξης του P ορίζεται ώς ένα νέο σημείο $R = k \cdot P = P + P + \cdots + P$.

2.2 ECDLP

Με βάση λοιπόν τον βαθμωτό πολλαπλασιασμό ορίζουμε το διακριτό πρόβλημα του λογαρίθμου σε ελλειπτικές καμπύλες ως εξής:
Έστω $Q = k \cdot P$ όπου Q, P γνωστά σημεία της ελλειπτικής καμπύλης και k ένας ακέραιος. Το k ονομάζεται διακριτός λόγαριθμος του Q στη βάση P και ζητούμενο του προβλήματος είναι ο υπολογισμός του.

2.3 Elliptic curve Diffie-Hellman (ECDH)

Το σχήμα ανταλλαγής κλειδιού Diffie-Hellman για ελλειπτικές καμπύλες ακολουθεί την ίδια λογική με το Diffie-Hellman και στηρίζεται στο ECDLP. Η διαδικασία που ακολουθείται παρουσιάζεται παρακάτω:
Αρχικά επιλέγονται δημόσια ένα πεπερασμένο σώμα F_p, μία ελλειπτική καμπύλη πάνω σε αυτό το σώμα και ένα σημείο G αυτής (domain parameters).
Έπειτα οι χρήστες Α και Β κάνουν τα παρακάτω:

- Επιλέγουν τυχαία έναν αριθμό d_A και d_B αντίστοιχα για τους οποίους ισχύει ότι $d < ord(G)$ και $d_B < ord(G)$.
- Υπολογίζουν το $Q = d_A \cdot G$ και $Q = d \cdot G$ με χρήση βαθμωτού πολλαπλασιασμού.
- Έχοντας σχηματίσει ένα ζεύγος public-private key (Q, d) και (Q_B, d_B) αντίστοιχα δημοσιεύουν τα Q_A, Q_B.
- Ο χρήστης Α υπολογίζει το $K = d_A \cdot Q_B$ και ο χρήστης Β το $K = \cdot Q_A$.
- Έτσι τελικά και οι 2 έχουν υπολογίσει το $K = d_A \cdot d_B \cdot Q = d_B \cdot d_A \cdot Q$, χωρίς να είναι εφικτό για κάποιον τρίτο να το υπολογίσει χωρίς να λύσει το πρόβλημα του διακριτού λογαρίθμου για ελλειπτικές καμπύλες.

2.4 Elliptic curve digital signature algorithm (ECDSA)

3 Υλοποίηση ενός συστήματος κρυπτογραφίας βασισμένο σε ελλειπτικές καμπύλες

3.1 Επιλογή καμπύλης και παραμέτρων

Ένας από τους κύριους λόγους χρησιμοποιήσης ελλειπτικών καμπυλών για υλοποίηση συστημάτων κρυπτογραφίας είναι ότι μπορούν να προσφέρουν τον ίδιο βαθμό ασφάλειας με συστήματα όπως το RSA ή το Diffie-Hellman με πολύ μικρότερο μήκος κλειδιού. Έτσι μειώνεται το υπολογιστικό κόστος χωρίς να επηρεάζεται ο βαθμός ασφάλειας.

ECC	RSA	Αναλογία	AES
163	1024	1:6	
256	3072	1:12	128
384	7680	1:20	192
512	15360	1:30	256

Για το λόγο αυτό τα συστήμα κρυπτογραφίας βασισμένα σε ελλειπτικές καμπύλες χρησιμοποιούνται ευρέως σε συσκευές με περιορισμένες υπολογιστικές δυνατότητες και σε συσκευές που απαιτείται χαμηλή κατανάλωση ενέργειας, όπως κινητά για παράδειγμα.

3.2 Επιλογή παραμέτρων

Για την αποφυγή επιθέσεων προς το κρυπτοσύστημα απαιτείται κατάλληλη επιλογή των παραμέτρων αυτού. Οι παράμετροι αυτοί είναι:

Αναφορές

[1] Don Johnson, Alfred Menezes, Scott Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, *Certicom Research*.

[2] Frank Pfenning, *Supplementary Notes on Futures*, November 2002.