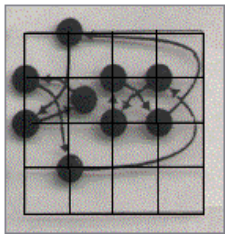
Η μέθοδος και το κρυπτοσύστημα των ελλειπτικών καμπυλών

Νίκος Λυγερός

Στο πρώτο μέρος της διάλεξης κάνουμε μια ολική παρουσίαση της μεθόδου παραγοντοποίησης μέσω τω ελλειπτικών καμπυλών, εξετάζοντας όλες τις περιπτώσεις στο κλασικό και πεπερασμένο επίπεδο. Μετά τη παρατήρηση του Lagrange, παρουσιάζουμε το θεώρημα του Hasse και αναλύουμε με παραδείγματα τη εφαρμογή της μεθόδου του Lenstra και τα καλύτερα αποτελέσματα των Curry, Lygeros & Mizony, Izum Dodson και Backstrom. Στο δεύτερο μέρος μελετούμε τις ειδικές και τις γενικές επιθέσεις τω κρυπτοσυστημάτων του τύπου Diffie και Hellman που βασίζονται στις επιλύσεις των προβλημάτων IFP, DL και ECDLP έτσι ώστε να εντοπίσουμε τους κινδύνους όσον αφορά την ασφάλεια της κρυπτογράφισης ειδικ για το πρόβλημα του διακριτού λογάριθμου των ελλειπτικών καμπυλών με τη ρ-μέθοδο του Pollard.



Εισαγωγή

Το 1985 ο Lenstra ανακάλυψε έναν αλγόριθμο παραγοντοποίησης που χρησιμοποιεί τις ελλειπτικέ καμπύλες.

Ελλειπτικές καμπύλες

Σύνολο των σημείων του επιπέδου από το οποίο οι συντεταγμένες ικανοποιούν την εξίσωση:

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

Οι παράμετροι α και b είναι ακέραιοι αριθμοί του τύπου $4a^3 + 27b^2 \neq 0$

Ιδιότητες

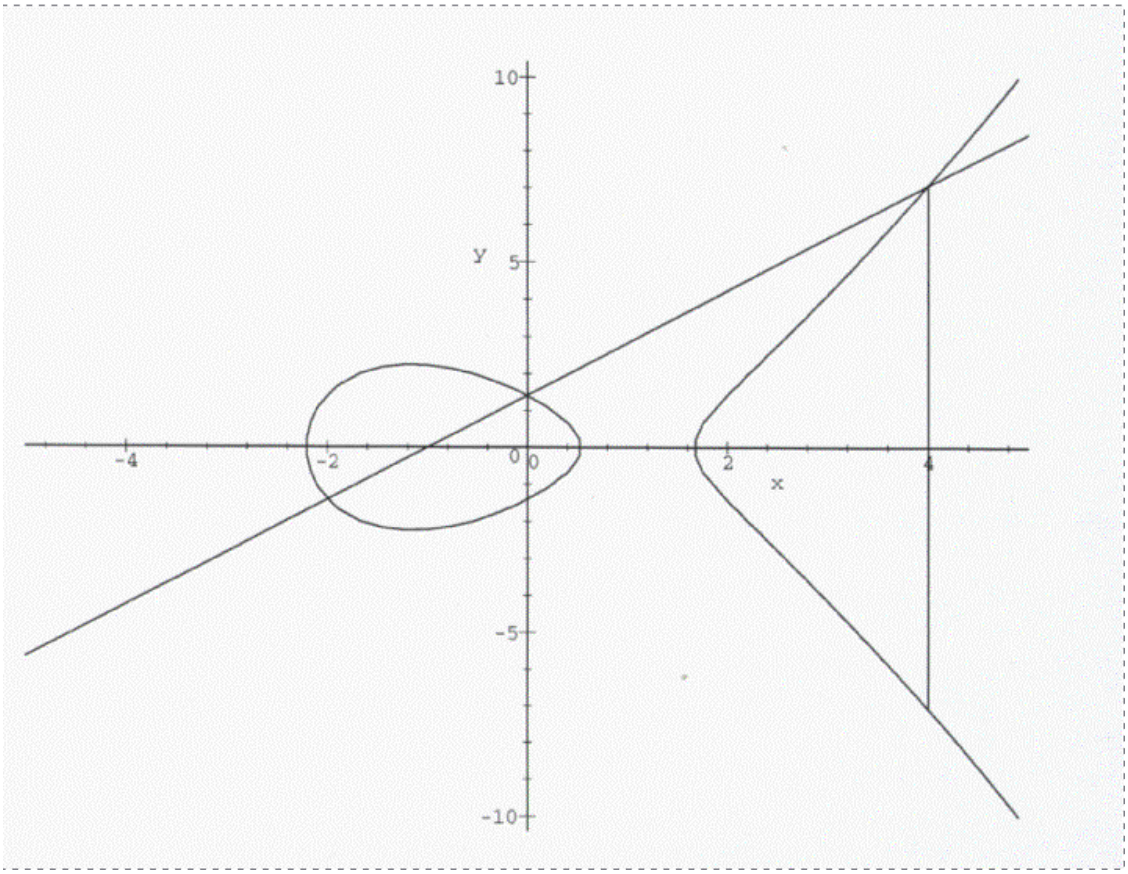
Πρόσθεση σημείων: $P_1(x_1, y_1)$ και $P_2(x_2, y_2)$

Παρατήρηση : $-P_1$ θα είναι $(x_1, -y_1)$

Έστω $y^2 = x^3 + ax + b$ μια ελλειπτική καμπύλη και $P_1(x_1, y_1)$ και $P_2(x_2, y_2)$ δύο σημεία της ελλειπτικής καμπύλης.

Η ευθεία που περνά από τα σημεία $P_1(x_1, y_1)$ και $P_2(x_2, y_2)$ είναι $y = \alpha x + \beta$

όπου $\alpha = \frac{y_1 - y_2}{x_1 - x_2}$ και $\beta = y_1 - \alpha x_1$



\

Εκφυλισμένη περίπτωση

Εάν $P_1(x_1, y_1) = P_2(x_2, y_2)$ τότε $\lambda = \frac{3x_1^2 + a}{2y_1}$

Αρκεί ο υπολογισμός της παραγώγου και εξίσωση της εφαπτόμενης της ελλειπτικής καμπύλης

Γενική περίπτωση

Εάν $P_1(x_1,y_1) \neq P_2(x_2,y_2)$ τότε $x^3+ax+b=(\alpha x+\beta)^2$ διότι $y=\alpha x+\beta$

$$x^3-\alpha^2x^2+x(a+2\alpha\beta)+\beta^2+b=0$$

Παρατήρηση: $x_1+x_2+x_3=\alpha^2$ (πρόσθεση του Newton)

Εδώ λ=α (παράμετρος του υπολογισμού) συνεπώς

$$x_3=-x_1-x_2+\lambda^2$$

και $y_3=-y_1+\lambda(x_1-x_3)$

διότι παίρνουμε το συμμετρικό σημείο σε σχέση με τον άξονα των πραγματικών.

Επιπλέον προσθέτουμε το ουδέτερο στοιχείο Ο το οποίο έχει άπειρες συντεταγμένες.

Modular Calculus

$y^2=x^3+ax+b \mod p$ και $4a^3+27b^2\neq 0 \mod p$

Παράδειγμα: εάν p=5, a=1, b= -1 και $P_1(1,1)$ και $P_2(2,2)$ τότε $P_3=P_1+P_2=(3,2)$

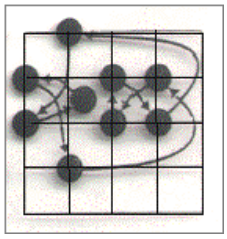
Το σύνολο E(p) των σημείων της ελλειπτικής καμπύλης modulo p είναι πεπερασμένο.

Εύκολο: $|E(p)|\leq (p-1)^2$

Δύσκολο: $p-2\sqrt{p}+1\leq|E(p)|\leq p+2\sqrt{p}+1$ (Θεώρημα του Hasse)

Παράδειγμα: εάν α=1, b=4 τότε E(5) έχει 9 σημεία

(3,3), (3,2), (0,3), (0,2), (1,4), (1,1), (2,3), (2,2) και Ο



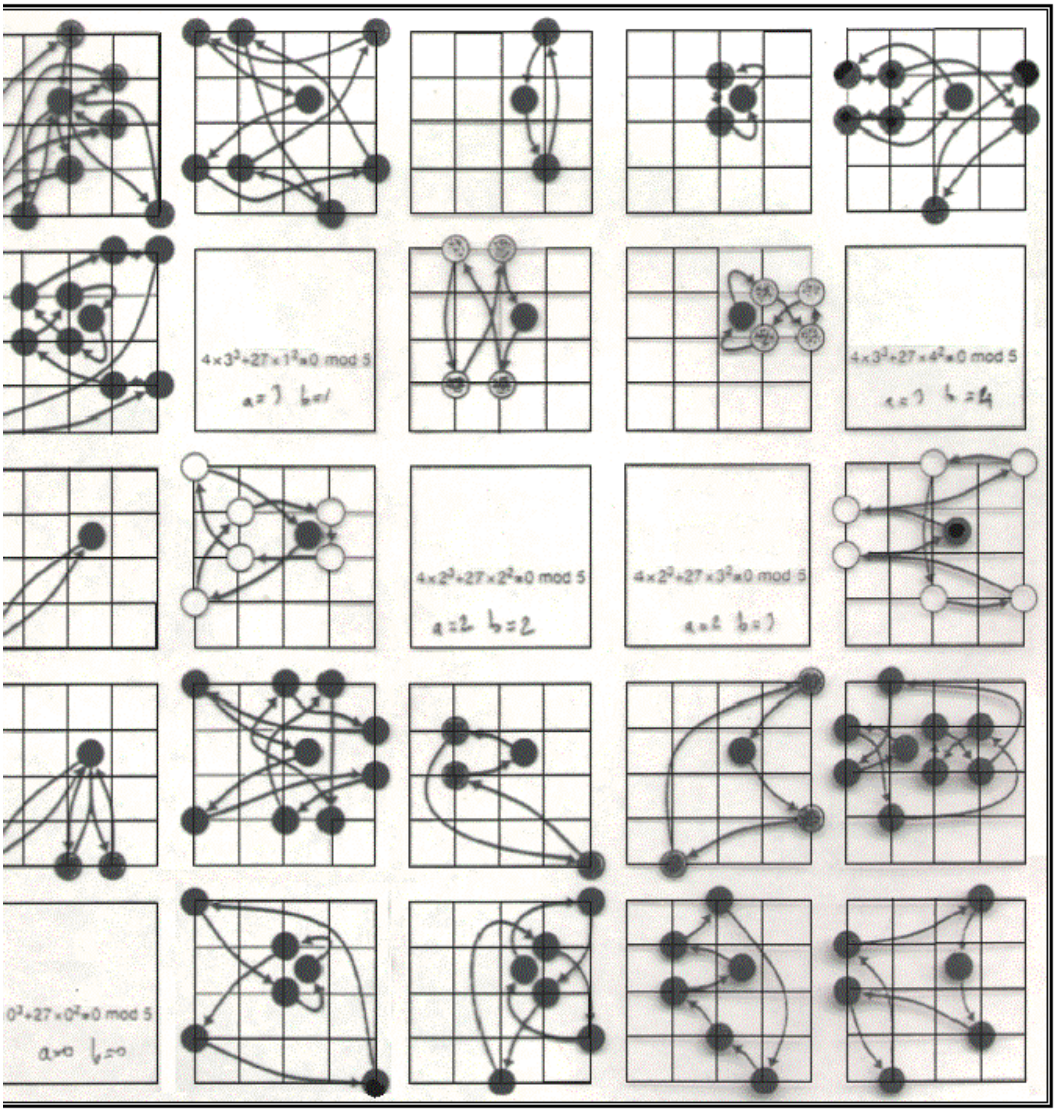
Παρατήρηση του Lagrange

Εάν προσθέσουμε n (τάξη της πεπ ερασμένης ομάδας) φορές ένα στοιχείο της ομάδας με τον ευατό του τ καταλήγουμε στο ουδέτερο στοιχείο
π.χ. x = (0,3) , x+x, x+x+x, …

(0,3) ➔ (1,1)➔ (3,3) ➔ (2,2) ➔ (2,3) ➔ (3,2) ➔ (1,4) ➔ (0,2) ➔ O (κύκλος)

Σύνολο των ελλειπτικών καμπυλών **E**(p)

Παράδειγμα : p=5 ⇒ 20 ελλειπτικές καμπύλες για 25 θεωρητικά εφυκτές


4×3³+27×1²≠0 mod 5
a=1 b=1
4×3³+27×4²≠0 mod 5
a=1 b=4
4×2³+27×2²≠0 mod 5
a=2 b=2
4×2³+27×3²≠0 mod 5
a=2 b=1
0³+27×0²≠0 mod 5
a=0 b=0

Υπολογισμός (Δυαδικό κόλπο)

P = (1, 1), 2P = (2, 2), 4P = 2(2P) = (0, 2), 8P = 2(4P) = (1, 4)
και 9P = 8P+P = (1,4)+(1,1) = O (ουδέτερο σημείο)

Ιδέα : 2P, 4P,…, 2^* P και τελική πρόσθεση

Παράδειγμα παραγοντοποίησης του 35 με το 5

Εστω a=1 και b=-1 τότε $4a^3 + 27b^2 \equiv 4+27 \equiv 31 \neq 0 \bmod 35$

Επιλογή του k (εξήγηση) k=9

Υπολογισμός του 9P

P= (2, 2), 2P = (0, 22), 4P = (16, 19), 8P = (7, 13)
και 9P = 8P+P= (7, 13) + (2, 2)

υπολογισμός του λ : 7-2≡5 mod 35

όμως το 5 δεν έχει αντίστροφο ως προς το 35 συνεπώς 5 | 35

Εξήγηση

|E(p)|=9 και 5 διαιρέτης του 35

Εις άτοπο επαγωγή

Προβολή mod 5

$$P_1 \in E(35) - - - - - - - - - - - - - > P_2 \in E(5)$$
$$9P_1 \in E(35) - - - - - - - - - - - - - > 9P_2 \in E(5)$$

Υπολογισμός του λ — Ουδέτερο στοιχείο (Lagrange)
Πεπερασμένες συντεταγμένες — Απειρες συντεταγμένες

Ατο

Παρατήρηση : ο χρόνος του υπολογισμού εξαρτάται από το μέγεθος του διαιρέτη.

PEKOP

	digits	factor	from	B1/B2	sigma	date	who
1	58	3213162276640339413566047915418064969550383692549981333701	8*10^141-17	3897500	2735675386	2003-Nov-01	R. Backstrom
2	57	167560816514084819488737767976263150405095191554732902607	2^997-1	44e6	6329517009540700	2003-Jun-22	B. Dodson
3	56	69787377067722881486602094502761253930262932578924438539	2^827+1	43e6	4029008539	2003-Dec-26	K. Aoki
4	55	72308801275268216939250595089720829527021330045523462 81	629^59-1	45e6	267937500	2001-	M. Izumi

						Oct-06	
5	55	52149924885212223606234700910452567496792505267107001 89	V(54,1,73)	43e6	3836151505	2003-Dec-10	D. Broadhurst
6	55	11391512582610346158801351068604464795264829590890616 29	XY(93,56)	30e6	556090596	2002-Dec-13	P. Gaudry
7	54	48406125427687836812572687078918023199596487009491693 7	(6^43-1)^42+1 [*]	15e6	599841120	1999-Dec-26	Lygeros/Mizony
8	54	47735083352247625882670527467031708214789373719349715 1	3^577-1	43e6	1939606094	2004-May-10	K. Aoki
9	54	13393670279561254503325313887286327664929946808958241 7	C(341,141)+1	11e6	1335265706	2002-Mar-19	C. Casey
10	54	11394465185665510779499610315004193933399392623012319 1	(3^64-1)^63+1	15e6	718797804	2000-Mar-21	Lygeros/Mizony

Public-key

Από το 1976 που εφευρέθηκε η public-key κρυπτογραφία από τους W. Diffie και M. Hellman, κρυπτοσυστήματα βασίζονται πάνω στη δυσκολία επίλυσης ενός μαθηματικού προβλήματος. Με τα χρόν όμως πολλά από αυτά τα κρυπτοσυστήματα απεδείχτηκαν μη σίγουρα ή μη πρακτικά. Τώρα μόνο τρία εί πλέον ανταγωνιστικά.

1. Integer factorization problem (IFP)

2. Discrete logarithm problem (DLP)

3. Elliptic curve discrete logarithm problem (ECDP)

Πρέπει να επιημάνουμε ότι κανένα από αυτά τα κρυπτοσυστήμαα δεν αποδείχτηκε προς το παρόν <<άτρωτο με την έννοια ότι δεν μπορεί να λυθεί με αποτελεσματικό τρόπο. Ενώ αυτό γίνεται μέσω των κβαντικ υπολογιστών (θεώρημα του Shor 1994).

Επιθέσεις των κρυπτοσυστημάτων

Οι ειδικές επιθέσεις εκμεταλλεύονται τα χαρακτηριστικά των αριθμών.
Οι γενικές επιθέσεις εξαρτόνται μόνο από το μέγεθος των αριθμών.

Ο αλγόριθμος των ελλειπτικών καμπυλών εξαρτάται από το μέγεθος των πρώτων παραγόντων του αριθμού τείνει να βρίσκει πρώτους αριθμούς μικρού μεγέθους. (εώς 60 ψηφία)

Το πρόβλημα του διακριτού λογάριθμου των ελλειπτικών καμπυλών

Εστω μια ελλειπτική καμπύλη E πάνω στο πεπερασμένο σώμα F_q ($q = 2^m$ ή $q \in \Pi$), $P \in E(F_q)$ σημείο τάξης n, κ
ένα $Q \in E(F_q)$ σημείο, να βρείτε τον ακέραιο l, $0 \le l \le n-1$ που να ικανοποιεί Q=lP όταν υπάρχει.

Με βάση τη δυσκολία αυτού του προβλήματος οι N. Koblitz και V. Miller ανέπτυξαν το 1985 ένα προτόκο
κρυπτοσυστήματος.

Ο Pohlig και ο Hellman απέδειξαν ότι η εύρεση του αριθμού l μπορεί να γίνει μέσω των πρώτων παραγόντ
του n. Άρα για να είναι πιο ασφαλές το κρυπτοσύστημα πρέπει να επιλέξουμε έναν αριθμό n που να εί
πρώτος αριθμός.

Ο καλύτερος αλγόριθμος για την επίλυση του προβλημάτος είναι η Pollard ρ-μέθοδος. Οι Gallant, Lambert κ
Vanstone με τους Wiener και Zuccherato έδειξαν ότι έχει $\frac{\sqrt{\pi n}}{2}$ βήματα όπου ένα βήμα είναι μια πρόσθεση σ
ελλειπτικές καμπύλες.

Το 1993, οι van Oorschot και Wiener απέδειξαν ότι η Pollard ρ-μέθοδος μπορεί να μετατραπεί σε παράλλη
αλγόριθμο.

Κριτικές ελλειπτικές καμπύλες

Όπως το 1991, οι Menezes, Okamoto και Vanstone απέδειξαν ότι το πρόβλημα μπορεί να απλοποιηθεί με
υπεριδιόρρυθμες ελλειπτικές καμπύλες μέσω του δείκτη υπολογισμού, αποφεύγουμε να τις χρησιμοποιούμε σ
κρυπτοσυστήματά μας.

Το ίδιο ισχύει και με τις ανώμαλες ελλειπτικές καμπύλες, οι οποίες έχουν ακριβώς q σημεία πάνω στο F_q. Κ
όπως με τις ιδιόρρυθμες υπάρχει για τις ανώμαλες, ένα εύκολο τες εντοπισμού της ιδιότητας αυτής.

Για τις καμπύλες του Koblitz μια ειδική κλάση ελλειπτικών καμπυλών πάνω στο F_{2^m} με συντελεστές που ανήκο
στο F_2 μπορεί να βρεθεί ένας γρηγορότερος αλγόριθμος επίλυσης του προβλημάτος. Αν όμως είναι αρκε
μεγάλος (m>160) τότε η επιτάχυνση είναι σχετικά ασήμαντη.

Hardware Attacks >> Software Attacks

Και στις δύο περιπτώσεις όμως τα αποτελέσματα πρέπει να επαναληφτούν για κάθε ελλειπτική καμπύλη τ χρήστη.

Symmetric-key cipher και Elliptic Curve Method

1. Ερευνα για k-bit symmetric-key cipher = Ερευνα για 2k-bit key elliptic curve method
2. Οι symmetric-key cipher και Pollard είναι παραλλελήσημοι με γραμμική επιτάχυνση.
3. Βήμα ECM >> Βήμα S-k cipher
4. Το σπάσιμο του κώδικα έχει το ίδιο αποτέλεσμα.

Επιλογές σωμάτων και ελλειπτικών καμπυλών

1. Επιλογή πεπερασμένου σώματος

Πολυπλοκότητα (F_{2^m}) = Πολυπλοκότητα (F_q)

όπου $q \in \Pi$

(προς το παρόν)

2. Παρουσίαση

α. Optimal normal basis representation

β. Polynomial basis representation

Μέσω των πινάκων αλλαγής βάσης τα α. και β. Είναι ισοδύναμα άρα δεν επηρεάζουν την πολυπλοκότητα τ κρυπτοσυστήματος.

3. Επιλογή της ελλειπτικής καμπύλης

ΟΧΙ ιδιόρρυθμες ή ανώμαλες ελλειπτικές καμπύλες

ΠΡΟΣΟΧΗ με τις καμπύλες του Koblitz για τα μικρά μεγέθη

Γενικό Συμπέρασμα

Το κρυπτοσύστημα των ελλειπτικών καμπυλών είναι πολυπλοκότερο

από τα κρυπτοσυστήματα του IFP (Integer Factorization Problem)
και DLP (Discrete Logarithm Problem)
άρα και πιο ασφαλές.