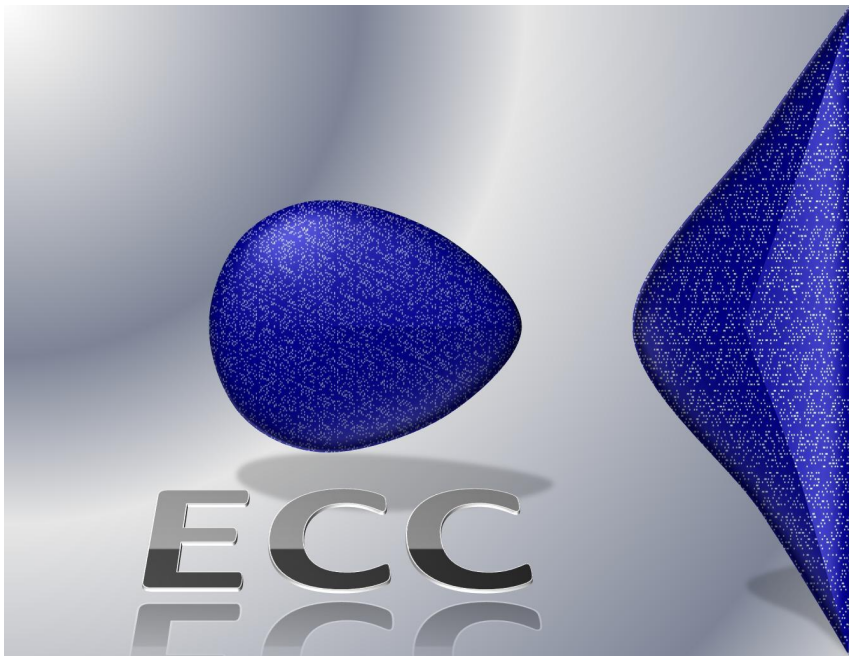
Κρυπτογραφία Ελλειπτικών Καμπυλών



Γενικά

- Μία μέθοδος κρυπτογραφίας δημοσίου κλειδιού
- Αντί για δακτύλιους της μορφής $\mathbb{Z}_n$ χρησιμοποιεί ελλειπτικές καμπύλες ορισμένες σε πεπερασμένα σώματα
- Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου
- Αυξημένη ασφάλεια με σχετικά μικρά μεγέθη κλειδιών

Ορισμός Ελλειπτικής Καμπύλης

Έστω ένα σώμα $\mathbb{F}$. Μία **ελλειπτική καμπύλη** $\mathcal{E}$ πάνω στο $\mathbb{F}$ ορίζεται από την εξίσωση:

$$y^2 + \alpha_1 xy + \alpha_3 y = \alpha_0 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_6,\ \alpha_i \in \mathbb{F}$$

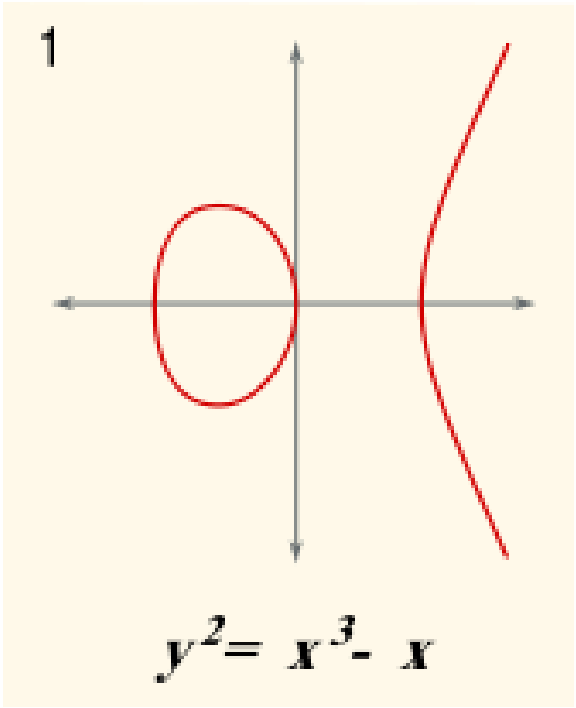
Η εξίσωση αυτή λέγεται εξίσωση Weierstrass.

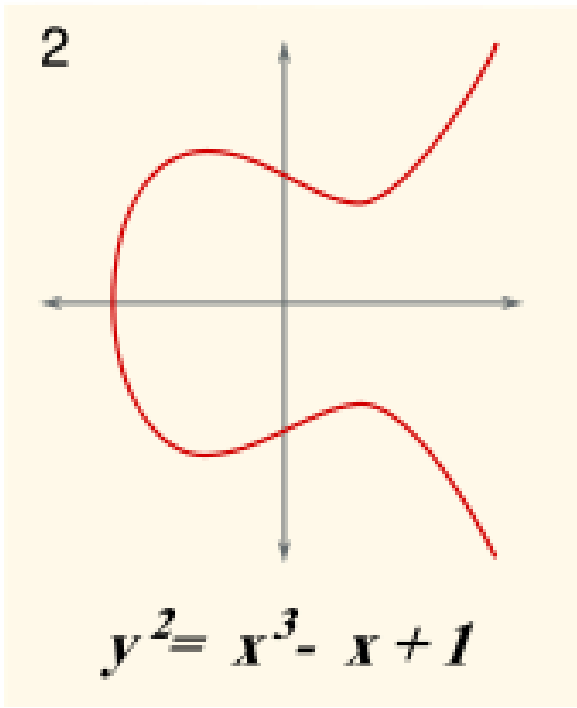
Σύνολο των ρητών σημείων της $\mathcal{E}$ είναι το σύνολο των $(x, y) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ τα οποία ικανοποιούν την εξίσωση Weierstrass μαζί με ένα σημείο $\mathcal{O}$ που ονομάζεται **σημείο στο άπειρο**.
Το σύνολο των σημείων της ελλειπτικές καμπύλης συμβολίζεται με $E(\mathbb{F}_q)$.
Τάξη του συνόλου αυτού είναι ο αριθμός των σημείων της καμπύλης $\#E(\mathbb{F}_q)$.

Σε ένα σώμα με χαρακτηριστική διάφορη του 2 ή του 3, η εξίσωση της ελλειπτικής καμπύλης παίρνει τη μορφή

$$y^2 = x^3 + \alpha x + b \text{ με } \alpha, b \in \mathbb{F}$$

Παραδείγματα ελλειπτικών καμπυλών





Έστω η ελλειπτική καμπύλη $\mathcal{E}$:

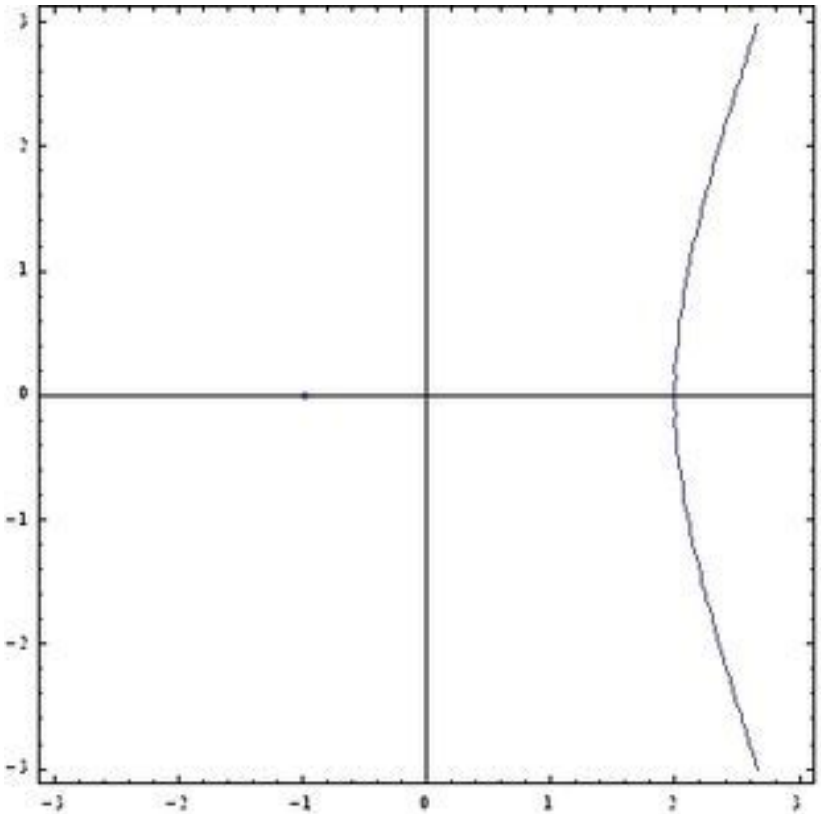
$$y^2 = x^3 + \alpha x + b$$

και μία ευθεία η οποία τέμνει την $\mathcal{E}$

$$y = \lambda x + c$$

Η ευθεία τέμνει την $\mathcal{E}$ σε τρία σημεία εκτός από την περίπτωση που ισχύει $4\alpha^3 + 27b^2 = 0$. Τότε η ελλειπτική καμπύλη λέγεται **ιδιάζουσα**

Παράδειγμα Ιδιάζουσας Ελλειπτικής Καμπύλης

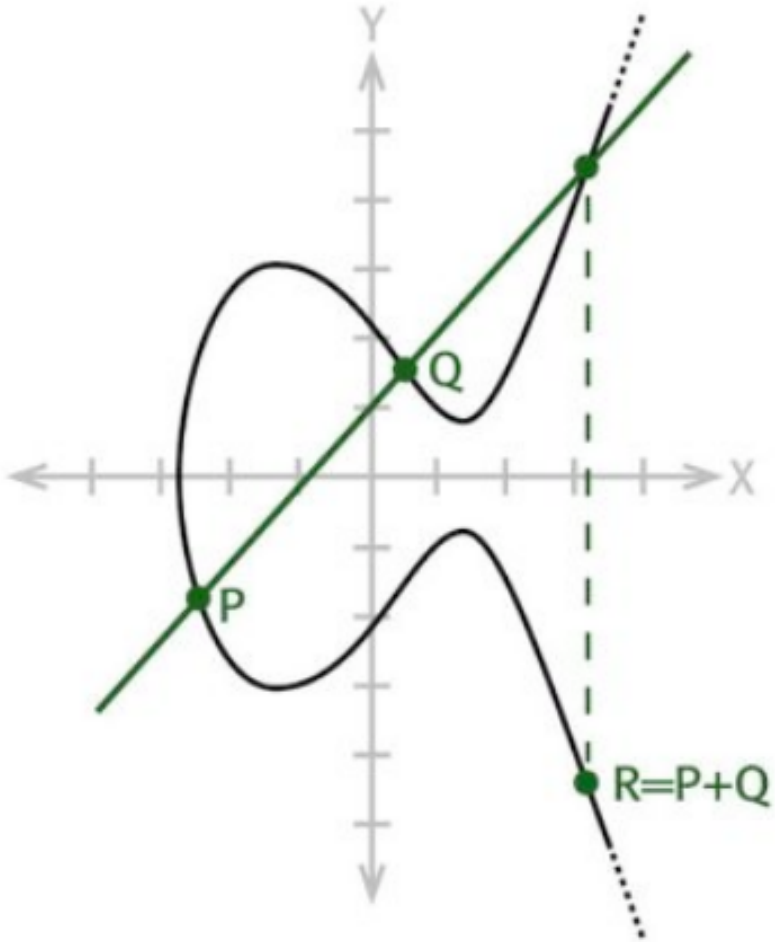


Το σύνολο των σημείων μιας ελλειπτικής καμπύλης $\mathcal{E}$*:* $y^2 = x^3 + \alpha x + b$ *πάνω σε ένα πεπερασμένο σώμα* $\mathbb{F}$ *με* $4\alpha^3 + 27b^2 \neq 0$ *μαζί με μία προσθετική πράξη αποτελούν μία* ***αβελιανή ομάδα*** *με το σημείο* $\mathcal{O}$ *να είναι το ουδέτερο στοιχείο.*

Ορισμός της πρόσθεσης

Έστω δύο σημεία της καμπύλης P, Q. Φέρνουμε την ευθεία που διέρχεται από αυτά και βρίσκουμε το τρίτο σημείο R που η ευθεία αυτή τέμνει την ελλειπτική καμπύλη. Το άθροισμα των $P + Q$ ορίζεται ως το συμμετρικό του R ως προς τον άξονα X. Το σημείο αυτό ορίζεται και ως το αντίστροφο του R και συμβολίζεται με $-R$. Δηλαδή ισχύει: $P + Q = -R$.

Πρόσθεση



- Αν η ευθεία που διέρχεται από δύο σημεία δεν τέμνει την ελλειπτική καμπύλη σε τρίτο, τότε το άθροισμά τους είναι το $\mathcal{O}$. Μπορούμε να θεωρήσουμε πως το τρίτο σημείο τομής είναι το άπειρο.
- Ορίζουμε ως αντίθετο σημείο $-P$ του σημείου P το συμμετρικό σημείο του P ως προς τον άξονα x. Δηλαδή, εάν $P = (x, y)$ τότε $-P = (x, -y)$. Μία ελλειπτική καμπύλη είναι συμμετρική ως προς τον άξονα X επομένως αν το σημείο $P = (x, y)$ ανήκει στην $\mathcal{E}$ τότε και το αντίθετό του, δηλαδή το $-P = (x, -y)$ θα ανήκει στην $\mathcal{E}$.

- Το σημείο $\mathcal{O}$ είναι το ουδέτερο στοιχείο της πρόσθεσης. Ισχύουν:

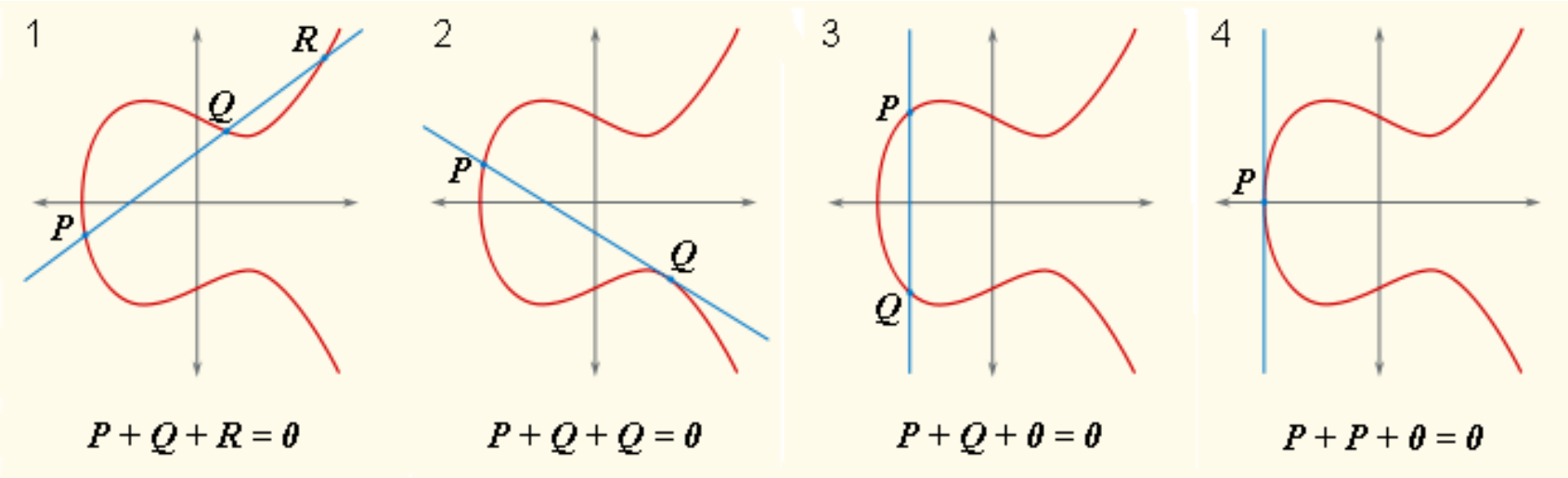
$$P + \mathcal{O} = \mathcal{O} + P = P$$
$$P + (-P) = \mathcal{O}$$

- Ισχύει:

$$P + Q = Q + P$$

- Στην περίπτωση που $P = Q$ δηλαδή τα δύο σημεία συμπίπτουν τότε η ευθεία που ορίζεται είναι η εφαπτόμενη στο σημείο $P = Q$. Το τρίτο σημείο τομής είναι το $\mathcal{O}$.

Πρόσθεση


1
R
Q
P
$P + Q + R = \theta$
2
P
Q
$P + Q + Q = \theta$
3
P
Q
$P + Q + \theta = \theta$
4
P
$P + P + \theta = \theta$

Θεώρημα Hasse

Έστω μία ελλειπτική καμπύλη ορισμένη στο πεπερασμένο σώμα $\mathbb{F}_q$. *Για το πλήθος των ρητών σημείων* $\#E(\mathbb{F}_q)$ *το οποίο ορίζει και την τάξη της ελλειπτικής καμπύλης ισχύει*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

Ο αριθμός $t = 2\sqrt{q}$ ονομάζεται ίχνος του Frobenius.
- Αν $t^2 = 0, q, 2q, 3q$ ή $4q$ τότε η ελλειπτική καμπύλη λέγεται **υπεριδιάζουσα**, διαφορετικά λέγεται **μη-υπεριδιάζουσα**.
- Αν $t = 1$ τότε η καμπύλη ονομάζεται **μη-ομαλή**.

Θεώρημα

Έστω μία ελλειπτική καμπύλη ορισμένη στο πεπερασμένο σώμα $\mathbb{F}_q$. *Το σύνολο* $E(\mathbb{F}_q)$ *είναι ισομορφικό με το* $C_{n_1} \oplus C_{n_2}$ *όπου* C_n *είναι κυκλική ομάδα τάξης* n. *Τα* n_1, n_2 *είναι μοναδικά και ισχύουν* $n_2 | n_1$ *και* $n_2 | q - 1$.

- Το πλήθος των σημείων της ελλειπτικής καμπύλης είναι $\#E(\mathbb{F}_q) = n_1 n_2$.
  Αν $n_2 = 1$ τότε το $E(\mathbb{F}_q)$ είναι κυκλική ομάδα.
  Αν $n_2 > 1$ τότε λέμε πως το σύνολο $E(\mathbb{F}_q)$ είναι τάξης 2.
  Αν ο αριθμός n_2 είναι μικρός (π.χ. $n_2 = 2, 3,$ ή 4) τότε το $E(\mathbb{F}_q)$ λέμε ότι είναι σχεδόν κυκλικό.
- Αν ο αριθμός $\#E(\mathbb{F}_q)$ είναι πρώτος τότε το $E(\mathbb{F}_q)$ είναι κυκλική ομάδα.
- Το $E(\mathbb{Z}_p)$ αποτελεί κυκλική ομάδα.
- Αν το $E(\mathbb{F}_q)$ είναι κυκλική ομάδα τότε κάθε σημείο P της ελλειπτικής καμπύλης εκτός από το $\mathcal{O}$ είναι γεννήτορας του συνόλου $E(\mathbb{F}_q)$.

Το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες (ECDLP)

Ορισμος:*Έστω μία ελλειπτική καμπύλη* $\mathcal{E}$ *ορισμένη στο* $\mathbb{F}_q$ *και έστω δύο σημεία αυτής,* P, Q *με το* P *να είναι τάξης* n*. Το πρόβλημα του διακριτού λογαρίθμου είναι η εύρεση ακεραίου* $l, 0 \leq l \leq n-1$ *αν υπάρχει, τέτοιο ώστε*

$$lP = Q$$

Αλγόριθμοι επίλυσης του ECDLP

- **Naive algorithm** δηλαδή ο υπολογισμός των $P, 2P, 3P, ...$ μέχρι να βρεθεί το Q απαιτεί n βήματα στη χειρότερη περίπτωση
- **Αλγόριθμος Poling-Hellman** ο υπολογισμός του διακριτού λογαρίθμου l ανάγεται στον υπολογισμό του l *modulo* p για κάθε πρώτο παράγοντα p του n.
- **Μεθόδος ρ του Pollard** που απαιτεί $(\sqrt{\pi n})/2$ βήματα όπου κάθε βήμα είναι μία πρόσθεση σημείων ελλειπτικής καμπύλης.

- Για ελλειπτικές καμπύλες ορισμένες σε ένα υποσώμα $\mathbb{F}_{2_l}$ του $\mathbb{F}_{2_m}$ ο υπολογισμός του διακριτού λογαρίθμου στο $E(\mathbb{F}_{2_m})$ γίνεται σε $\sqrt{(\pi nl/m)}/2r$ βήματα.
- Αν για μία ελλειπτική καμπύλη ισχύει $\#E(\mathbb{F}_q) = q$ τότε αυτή ονομάζεται ανώμαλη. Στην περίπτωση αυτή ο διακριτός λογάριθμος υπολογίζεται σε πολυωνυμικό χρόνο.

Με εξαίρεση τις δύο αυτές περιπτώσεις δεν έχει βρεθεί αλγόριθμος με υπο-εκθετικό χρόνο για την επίλυση του ECDLP.

Το πρόβλημα Diffie-Hellman στις ελλειπτικές καμπύλες (ECDHP)

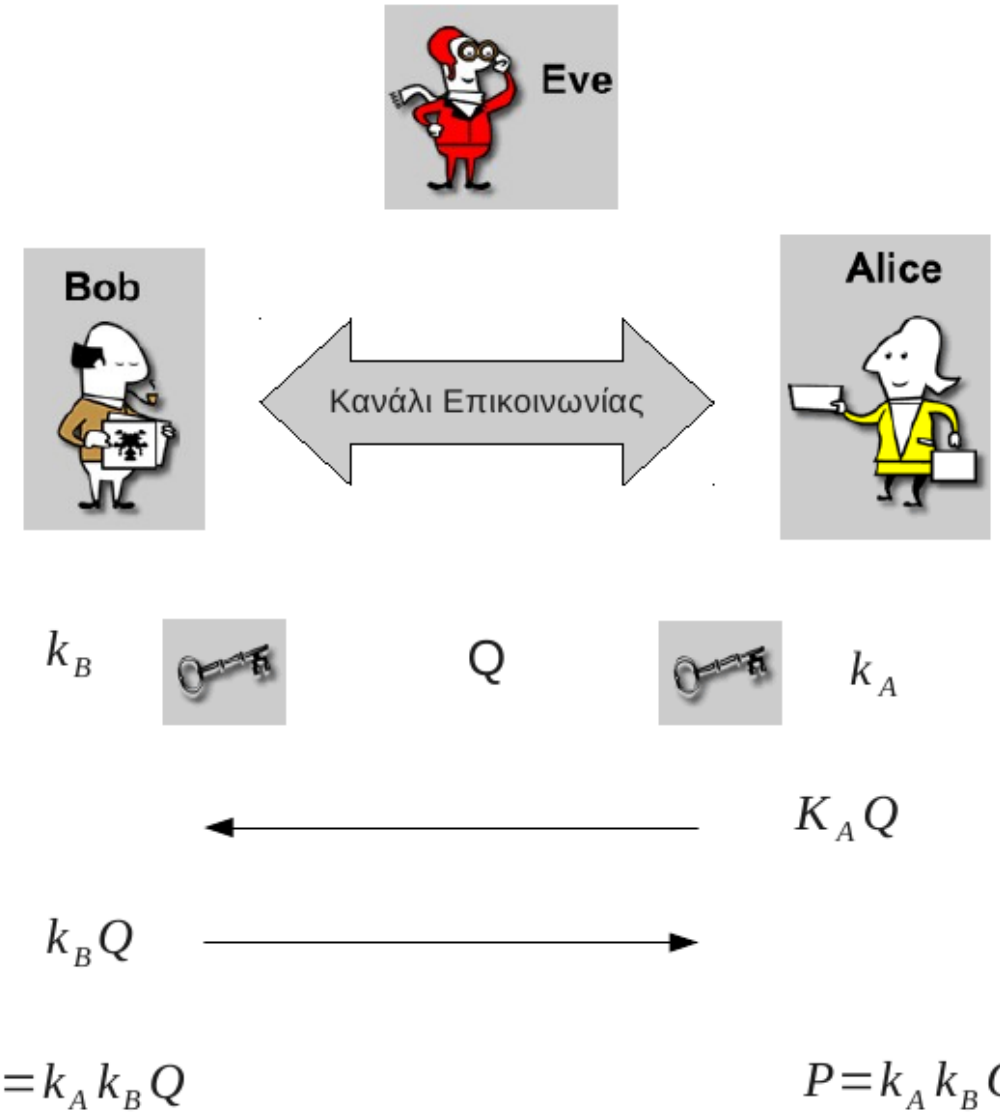
Ορισμός: *Έστω μία ελλειπτική καμπύλη $\mathcal{E}$ ορισμένη στο $\mathbb{F}_q$ και έστω τα σημεία $P, k_1P, k_2P \in E(\mathbb{F}_q)$ ζητείται το σημείο k_1k_2P.*

Έχει αποδειχθεί ότι αν το ECDLP δεν μπορεί να λυθεί σε υπο-εκθετικό χρόνο τότε ούτε το ECDHP μπορεί να λυθεί σε υπο-εκθετικό χρόνο.

Κρυπτοσυστήματα σε ελλειπτικές καμπύλες

Τα κρυπτοσυστήματα που βασίζονται στο πρόβλημα του διακριτού λογαρίθμου μπορούν να τροποποιηθούν έτσι ώστε να μπορούν να οριστούν πάνω στο σύνολο των σημείων μιας ελλειπτικής καμπύλης.

Το πρωτόκολο Diffie-Hellman στις ελλειπτικές καμπύλες



Το ανάλογο του κρυπτοσυστήματος El Gamal

k_B Ιδιωτικά Κλειδιά k_A

Q: Δημοσίως γνωστό

$k_A Q$ ←

$k_B Q$ →

Μήνυμα: m

m → P_m Σημείο της καμπύλης

$(C_1, C_2) = (k_A Q, P_m + k_A(k_B Q))$ ←

$$C_2 - k_B C_1 = P_m + k_A(k_B Q) - k_B(k_A Q) = P_m$$

Ασφάλεια

Τα Q και $k_B Q$ είναι δημόσια γνωστά.
Αν υπολογιστεί το k_B τότε το μήνυμα της Alice αποκρυπτογραφείται.
Η ασφάλεια του ανάλογου κρυπτοσυστήματος του El Gamal καθορίζεται από το κατά πόσο είναι επιλύσιμο το ECDLP.
Το αν μπορεί να λυθεί το ECDLP εξαρτάται από την επιλογή της ελλειπτικής καμπύλης και από το σημείο-βάση Q.

Επιθέσεις

- MOV Reduction ή MOV attack
- Η μέθοδος του Shanks:'baby-step giant-step'
- Polling-Hellman attack
- Η μέθοδος ρ του Pollard

Επιλογή Κατάλληλης Ελλειπτικής Καμπύλης

Γενικά, η τάξη της ελλειπτικής καμπύλης πρέπει να είναι

$$\#E(\mathbb{F}_q) = n \cdot p \text{ ή } \#E(\mathbb{F}_q) = p$$

όπου n μικρός ακέραιος και p μεγάλος πρώτος αριθμός.

Υπάρχουν τέσσερις τεχνικές:

- Με βάση το θεώρημα του Hasse
- Η καθολική Μέθοδος
- Complex Multiplication Method (CM)
- Τυχαία Επιλογή

Μήκος κλειδιού

Description	*RSA*	*ElGamal*	*ECC*
Can be broken with basic technologies	816 *bits*	816	128
Can be broken in short time	1008	1008	144
In theory adequate	1248	1248	160
Generally regarded as absolute minimum	1776	1776	192
Guarantees minimum security	2432	2432	224
Adequate except top secret documents	3248	3248	256
Adequate even for top secret documents	15424	15424	512

Υπολογιστικός χρόνος

	MHz	163 ECC	192 ECC	1024 RSAe	1024 RSAd	2048 RSAe	2048 RSAd
Ultra SparcII 400MHz	450	6.1	8.7	1.7	32.1	6.1	205.5
Strong ARM 200MHz	200	22.9	37.7	10.8	188.7	39.1	1273.8

Σχήμα: Υπολογιστικός χρόνος ECC-RSA(encryption-decryption) σε msec

Εφαρμογές του κρυπτοσυστήματος ελλειπτικών καμπυλών

- Έξυπνες κάρτες
- ασύρματες συσκευές όπως τα PDA
- Τηλέφωνα που υποστηρίζουν εφαρμογές multimedia
- Smart Phones