Υλοποίηση αταλλαγής κλειδιού DH και ψηφιακών υπογραφών βασισμένη σε ελλειπτικές καμπύλες

Νίκος Γιανναράκης
Ζωή Παρασκευοπούλου

Σχολή Ηλεκτρολόγων Μήχανικών και Μηχανικών Υπολογιστών
Εθνικό Μετσόβιο Πολυτεχνείο

27 Ιανουαρίου 2013

Κρυπτογραφία με ελλειπτικές καμπύλες

Why elliptic curve cryptography?

- Αυξημένη ασφάλεια με μικρότερα μεγέθη κλειδιών
- Μειωμένο υπολογιστικό κόστος
- Ιδανικές για φορητές συσκευές (κινητά κλπ.)

Ελλειπτικές καμπύλες στο $\mathcal{R}$

Ορισμός

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

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

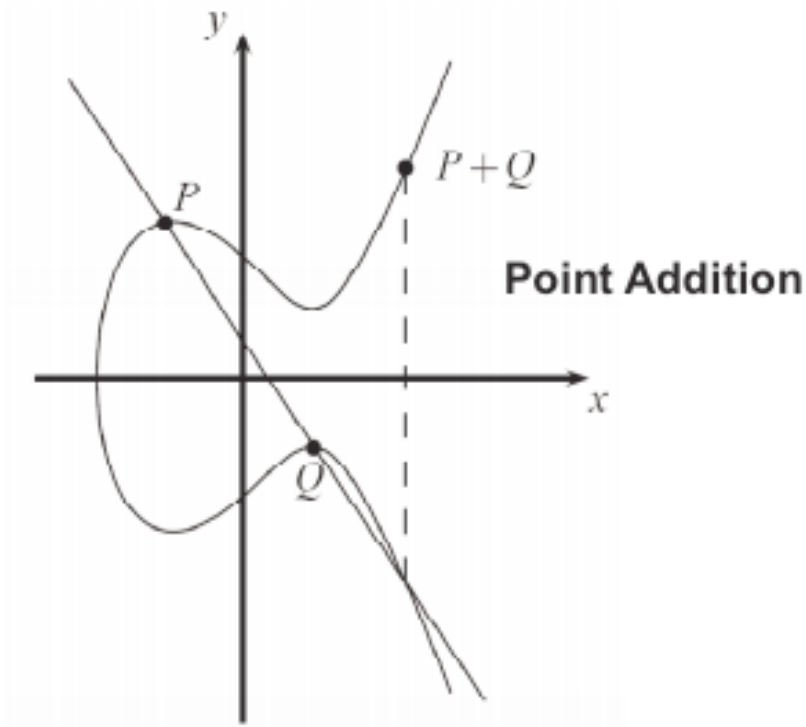
μαζί με ένα σημείο $\mathcal{O}$, το οποίο ονομάζουμε σημείο στο άπειρο.

Ορισμός πράξεων

- Πρόσθεση δύο σημείων P, Q
- Διπλασιασμός ενός σημείου P

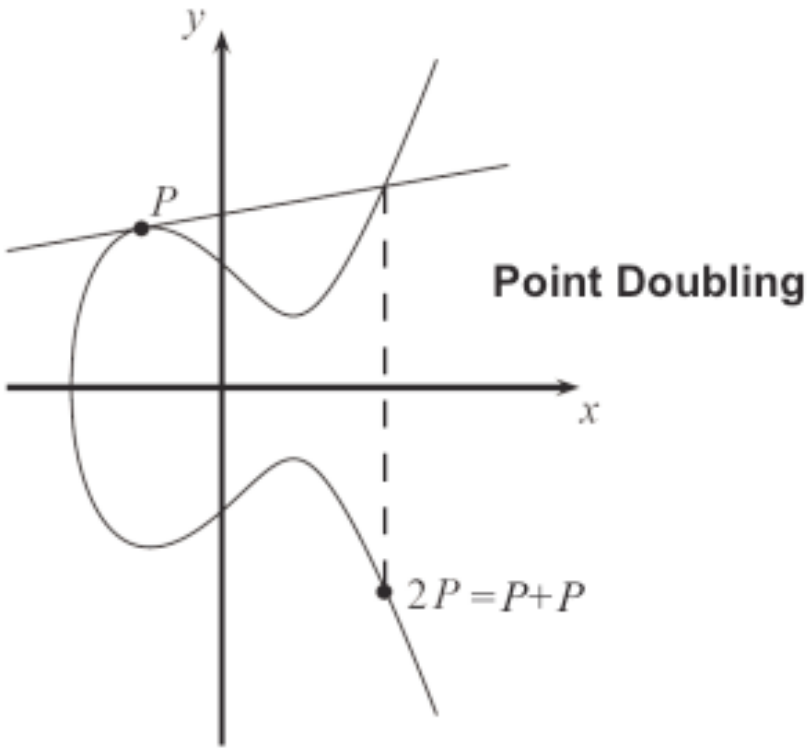
Πρόσθεση δύο σημείων πάνω σε ελλειπτικές καμπύλες στο $\mathcal{R}$

Η πρόσθεση δύο σημείων P, Q μπορεί να οριστεί γεωμετρικά



Διπλασιασμός σημείου πάνω σε ελλειπτικές καμπύλες στο $\mathcal{R}$

Ο διπλασιασμός ενός σημείου πάνω σε μία ελλειπτική καμπύλη ορίζεται γεωμετρικά σύμφωνα με το παρακάτω σχήμα



Προβλήματα

- Αργές πράξεις σε πραγματικούς αριθμούς
- Έλλειψη ακρίβειας

Ελλειπτικές καμπύλες πάνω από το $\mathbb{F}_p$ και το $\mathbb{F}_{2^m}$

Ορισμός

Διαλέγοντας $a, b \in \mathbb{F}_p$ και υπολογίζοντας τα σημεία (x, y) της καμπύλης $modulo\ p$ ορίζουμε μία ελλειπτική καμπύλη στο $\mathbb{F}_p$.

Πρόσθεση δύο σημείων πάνω σε ελλειπτικές καμπύλες στο $\mathbb{F}_p$

Η πρόσθεση δύο σημείων $R = P + Q$ σε μία ελλειπτική καμπύλη στο $\mathbb{F}_p$ ορίζεται αλγεβρικά:

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

Διπλασιασμός σημείου πάνω σε ελλειπτικές καμπύλες στο $\mathbb{F}_p$

Ο διπλασιασμός σημείου $R = 2P$ σε μία ελλειπτική καμπύλη στο $\mathbb{F}_p$ ορίζεται αλγεβρικά:

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

Βαθμωτός πολλαπλασιασμός πάνω σε ελλειπτικές καμπύλες στο $\mathbb{F}_p$

Με χρήση των παραπάνω πράξεων μπορούμε να ορίσουμε την πράξη του βαθμωτού πολλαπλασιασμού $R = k \cdot P$ όπου $l \in \mathbb{Z}$ και P ένα σημείο ελλειπτικής καμπύλης.

- Naive $P + P \ldots + P$
- Double-and-add (το ανάλογο του επαναλαμβανόμενου τετραγωνισμού)
- Windowed, Sliding-window, wNAF, Montogomery ladder ...

Verbatim

Example (Putting Verbatim)

```
\begin{frame}
\frametitle{Outline}
\begin{block}
{Why Beamer?}
Does anybody need an introduction to Beamer?
I don't think so.
\end{block}
% Extra carriage return causes problem with verbatim %
\end{frame}
```

Example of the `\cite` command to give a reference is below:
Example of citation using [?] follows on.

References

Author's name (1987)

Title of the paper.

Journal Name 55(4), 765 – 799.

The End