Cryptography & Encryption:6G7Z1011 : Elliptic Cryptography & Quantum Encryption

Keith Yates

March 15, 2019

Summary and Last Direction

1. We have covered the main encryption public key algorithms.
2. Today, we look at some of the newer encryption techniques, specifically
   a) Elliptic Curve Cryptography
   b) Quantum Crptography.
3. We explicitly construct $\mathbb{F}_{3^2}$.

Elliptic Curve Cryptography

We have a look at Elliptic Curve Cryptography, a newer approach to encryption that was developed after RSA, and will come to the fore in the next few years.
A misnomer: elliptic curves are not ellipses.
`http://www.maa.org/sites/default/files/pdf/upload_libra`

Why bother?

RSA is a widely-supported encryption technique with no feasible attack strategies. Elliptic curve cryptography also has no known attack strategies, but it has one big advantage Elliptic keys are smaller (reducing storage and transmission requirements) an elliptic curve group can use a 256-bit elliptic curve public key and it is believed to be as secure as 3072-bit RSA public key.
(same security, with a key a tenth of the length).

Elliptic Curves

An *elliptic curve* is a curve of the form

$$y^2 = x^3 + Ax + B \tag{0.1}$$

where A and B are parameters.

In a Nutshell

The RSA algorithm and the ElGamal algorithm involved us solving equations of the form

$$x^a = b \mod n. \tag{0.2}$$

The theory required us to develop a little of the structure theory of finite fields. Recall to each prime p there is one and only one field of size p^n, n a positive integer, and we wrote this $\mathbb{F}_{p^n}$.
Elliptic curve cryptogtaphy uses ideas from two dimensional geometry to create a new group structure that is used in encryption.

Example

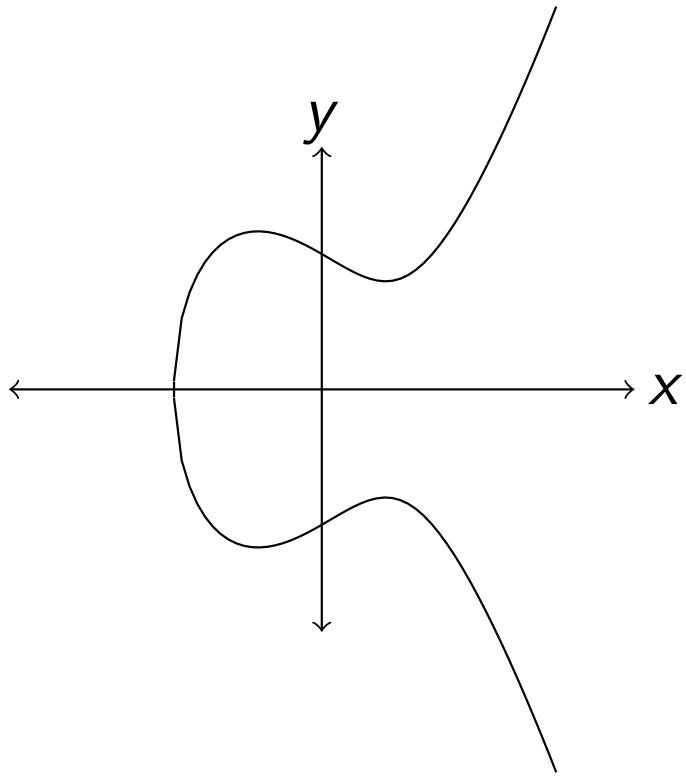

Figure: The elliptic curve $y^2 = x^3 + Ax + B$, $A = -3$, $B = 3$ $y^2 = x^3 - 3x + 3$.

Points on the Curve

The shape of the curve $y^2 = x^3 + Ax + B$ is dependent on A, B. For example consider the equation

$$y^2 = x^3 - 15x + 18. \tag{0.3}$$

Which of the following points lies on the curve in eqn. 0.3?

1. $P = (7, 16)$
2. $Q = (1, 2)$
3. $R = (2, 1)$

Just plug in the numbers

$P = (7, 16)$

We have

$$y^2 = x^3 - 15x + 18, \tag{0.4}$$

and setting $x = 7$ we find

$$x^3 - 15x + 18 = 7^3 - 15.7 + 18 = 256 \tag{0.5}$$

and $y = 16$ gives

$$y^2 = 256. \tag{0.6}$$

$Q = (1, 2)$

We have

$$y^2 = x^3 - 15x + 18, \tag{0.7}$$

and setting $x = 1$

$$x^3 - 15x + 18 = 1^3 - 15 + 18 = 4 \tag{0.8}$$

and $y = 2$

$$y^2 = 4. \tag{0.9}$$

Placing a Group Structure on the Curve

The new insight (Koblitz and Miller 1985) is that we can place a group structure on an elliptic curve. Recall a group consists of a set G and a binary operation $\circ : G \times G \to G$, $(a, b) \mapsto a \circ b$. The binary operation is required to satisfy the following properties:

1. $\circ$ is an associative operation, that is $a \circ (b \circ c) = (a \circ b) \circ c$.
2. There exists a $1 \in G$ such that $1 \circ g = g \circ 1 = g$ for all $g \in G$; the element 1 is termed the group identity.
3. To each $g \in G$ there exists a $g^{-1} \in G$ such that $g \circ g^{-1} = 1$; the element g^{-1} is termed the inverse of g.

Group addition $\oplus$

The group we construct will be abelian and in this case the group operation is usually denoted by $+$; however if you are given two points (a, b) and (c, d) in the plane $\mathbb{R}^2$ then $+$ is usually taken to mean

$$(a, b) + (c, d) = (a + c, b + d). \tag{0.10}$$

And that is not how we will define the group operation for an elliptic curve, we will use $\oplus$.

Group addition $\oplus$

Given two points on an elliptive curve P and Q we need to define their sum $R = P \oplus Q$, and when this is done we need to check all the axioms of a group are satisfied.

Group addition $\oplus$

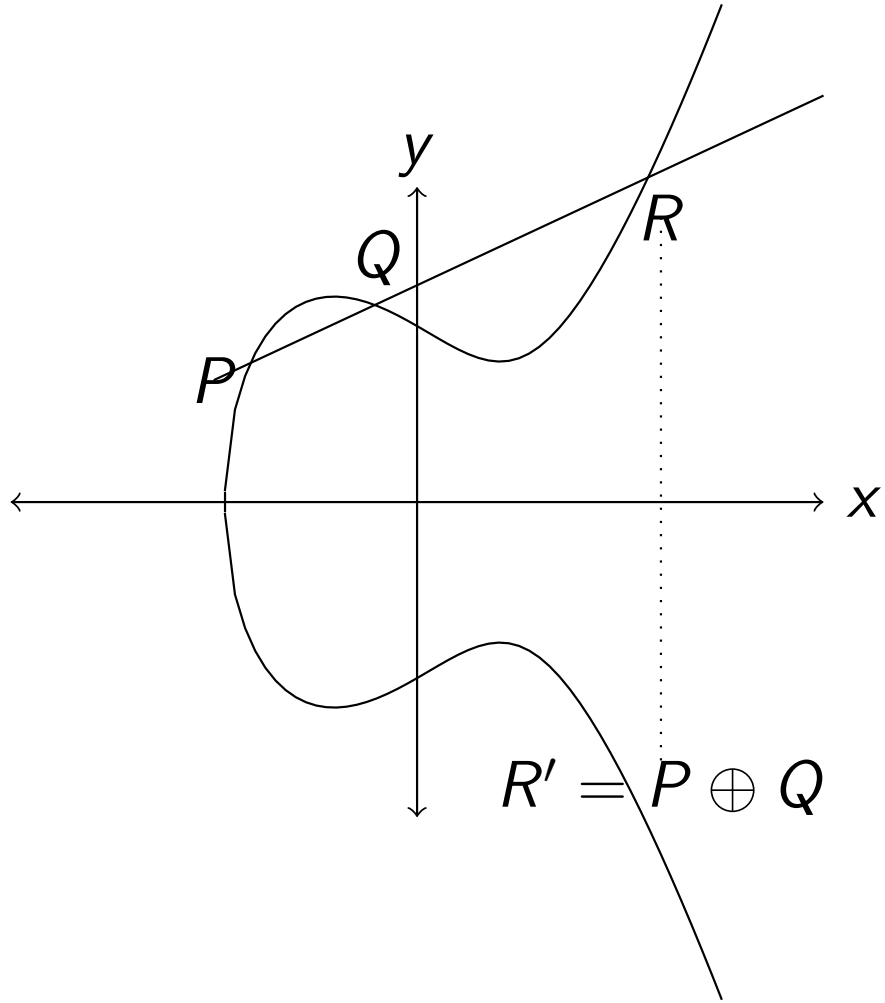

Figure: The elliptic curve $y^2 = x^3 + Ax + B$, $A = -3$, $B = 3$ $y^2 = x^3 - 3x + 3$.

Group addition in Words

Let points P and Q lie on the curve

1. Draw the straight line through P and Q it will will meet the curve at a third point R
2. Reflect R in the y-axis, this point is defined to be $P \oplus Q$.

Example

Let E be the elliptic curve

$$y^2 = x^3 - 15x + 18. \tag{0.11}$$

Let $P = (7, 16)$ and $Q = (1, 2)$. What is $P \oplus Q$?.
Give it a go —you need a little geometry

A bit more geometry

In case your mathematics is a little rusty, we need to describe the equation of the line that joins two points

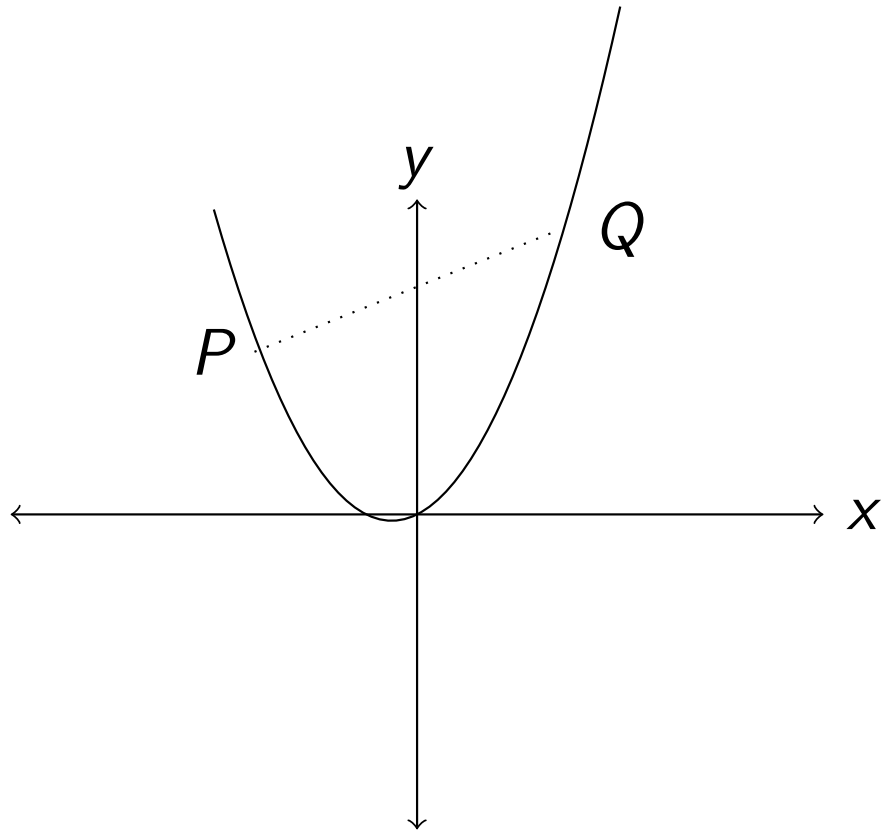

Figure: We require the equation of the straight line between points P and Q.

A little geometry

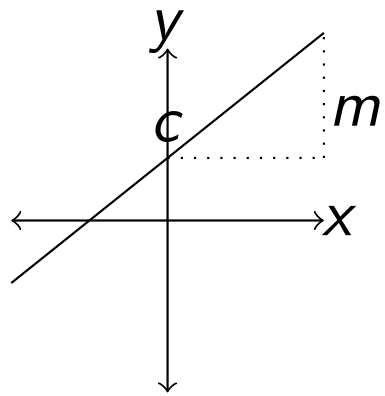

Figure: $y = mx + c$

Recall the equation of a line can be written

$$y = mx + c; \tag{0.12}$$

where m is the gradient of the line, and c is its intercept on the y axis. Consider points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.

Equation of Line

Using the gradient and intercept idea, if we know two points on the straight line (say) (x_1, y_1) and (x_2, y_2) then the line is described by the equation

$$y = y_1 + \frac{(y_2 - y_1)}{x_2 - x_1}(x - x_1) \tag{0.13}$$

So for $(7, 16)$ and $(1, 2)$ we deduce

$$y = 16 + \frac{(2-16)}{(1-7)}(x - 7) \quad \text{and rearranging} \quad y = \frac{7x}{3} - \frac{1}{3}. \tag{0.14}$$

Where are we now?

Recall we seek the point R, and we know P, Q and

$$y = \frac{7x}{3} - \frac{1}{3} \quad \text{and} \quad y^2 = x^3 - 15x + 18. \tag{0.15}$$

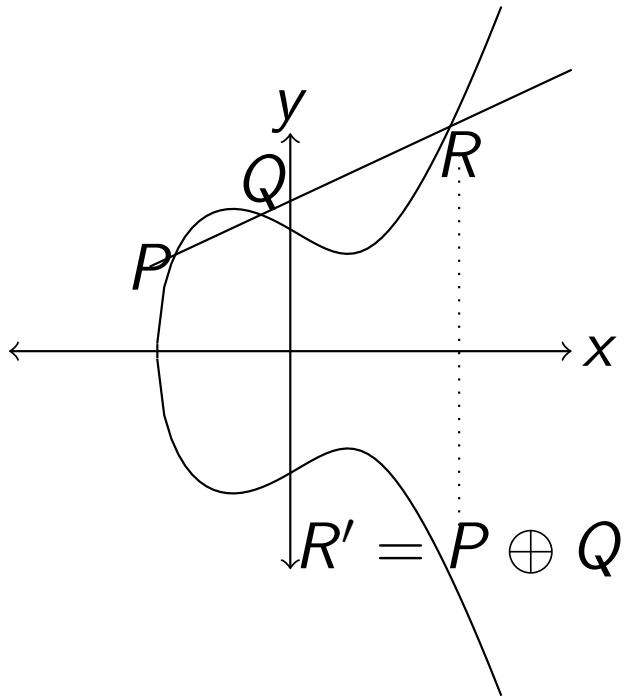

Figure: An elliptic curve

cubic equations

We seek the simultaneous solution of the two equations

$$y = \frac{7x}{3} - \frac{1}{3} \quad \text{and} \quad y^2 = x^3 - 15x + 18. \tag{0.16}$$

The general solution of a cubic is readily available online
`https://en.wikipedia.org/wiki/Cubic_functionGeneral_fo`

cubic equations

We seek the solution to

$$\left(\frac{7x}{3} - \frac{1}{3}\right)^2 = x^3 - 15x + 18 \tag{0.17}$$

Can we multiple it out and deduce the cubic please?

Some working out

$$\begin{aligned} \left(\frac{7x}{3} - \frac{1}{3}\right)^2 &= x^3 - 15x + 18 \\ \frac{49x^2}{9} - \frac{14x}{9} + \frac{1}{9} &= x^3 - 15x + 18 \\ 0 = \quad & x^3 - \frac{49}{9}x^2 - \frac{121}{9}x + \frac{161}{9} \end{aligned} \tag{0.18}$$

There is a general solution for a cubic, we already know two solutions $P = (7, 16)$ and $Q = (1, 2)$ thus

More Working Out

Two solutions are $P = (7, 16)$ and $Q = (1, 2)$ thus

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x + \frac{161}{9} = (x-7)(x-1)(x+\frac{23}{9}) \quad (0.19)$$

and $x = \frac{-23}{9}$ so

$$y = \frac{7x}{3} - \frac{1}{3} \quad \text{implies} \quad y = \frac{7.(-23)}{27} - \frac{3}{27} = \frac{170}{27}. \quad (0.20)$$

And finally reflecting the y point

$$P \oplus Q = \left(\frac{-23}{9}, \frac{-170}{27}\right) \quad (0.21)$$

Caveats

I have glossed over a few details:

1. We need to add an identity element $O_\oplus$ to the solutions (recall a group needs an identiry element, it is a group axiom) this is no problem $O_\oplus + P = P = P + 0_\oplus$.
2. If $P = Q$ we are more trouble, because there is no line between P and P, so we can not solve the equation as we did earlier.

Elliptic Curve Addition Algorithm

Consider

$$y^2 = x^3 + Ax + B \mod \mathbb{F}_p \tag{0.22}$$

and let P_1 and P_2 be solutions to eqn. 0.22.

1. If $P_1 = O_\oplus$ then $P_1 + P_2 = P_2$.
2. If $P_2 = O_\oplus$ then $P_1 + P_2 = P_1$.
3. Otherwise let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$
   a) If $x_1 = x_2$ and $y_1 = -y_2$ then $P_1 + P_2 = O_\oplus$
   b) Otherwise, define λ to be

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{if } x_1 \neq x_2, \quad \frac{3x_1^2 + A}{2y_1} \quad \text{if } x_1 = x_2 \tag{0.23}$$

set $x_3 = \lambda^3 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ and define

$$P_1 \oplus P_2 = (x_3, y_3). \tag{0.24}$$

Online

http://www.christelbach.com/eccalculator.aspx

Constructing $\mathbb{F}_{3^2}$

CW1 requires you construct $\mathbb{F}_{3^2}$ recall this is the unique field of size 3^2, and recalling the definition of a field

1. $\mathbb{F}_{3^2}$ is under addition an abelian group
2. the non-zero elements of $\mathbb{F}_{3^2}$ are under multiplication an abelian group.

So $\mathbb{Z}_9$ is not a field! Because

$$3 \times 3 = 0 \mod 9 \tag{0.25}$$

skew symmetric

A matrix M is termed skew-symmetric if its off-diagonal elements satisfy $M_{i,j} = -M_{j,i}$. A property of 2×2 skew-symmetric matrices with a single number on their diagonal is they commute. Please prove this

commutativity of skew-symmetric 2×2 matrices

In general multiplication of matrices need not be abelian however for skew-symmetric matrices we find

$$\begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -(x_1y_2 + x_2y_1) & (x_1x_2 - y_1y_2) \end{pmatrix}. \tag{0.26}$$

Constructing $\mathbb{F}_{3^2}$

The reason for proving the commutativity is that it saves us a lot of work, in particular when we work out the field table in the question sheet we know $AB = BA$ so we need only work out AB.

The following matrices are a field of cardinality nine over $\mathbb{Z}(3)$

$$a = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix},$$
$$d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix},$$
$$g = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad h = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}, \quad i = \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}. \tag{0.27}$$

Quantum Cryptography

Quantum Cryptography depends crucially on Heisenberg's uncertainity principle
`https://www.youtube.com/watch?v=a8FTr2qMutA`

Quantum Cryptography

Quantum Cryptography - does it lead to a one time pad?
https://www.youtube.com/watch?v=UiJiXNEm-Go

Quantum Cryptography

I think the most important idea here is that Eve