Elliptic Curves and the State of Survaillence

Aleksander Horawa

Imperial College London

November 24, 2015

Reference: Thomas C. Hales, *The NSA Back Door to NIST*, Notices of the AMS.

image credits: https://wordtothewise.com/

image credits: https://wordtothewise.com/

image credits: https://wordtothewise.com/

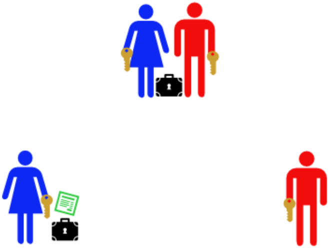


image credits: https://wordtothewise.com/

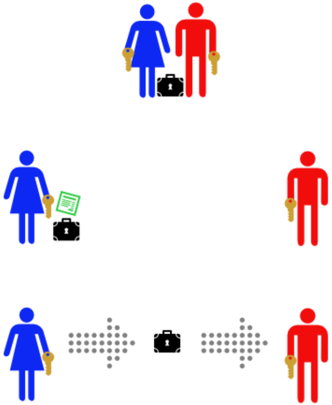


image credits: https://wordtothewise.com/

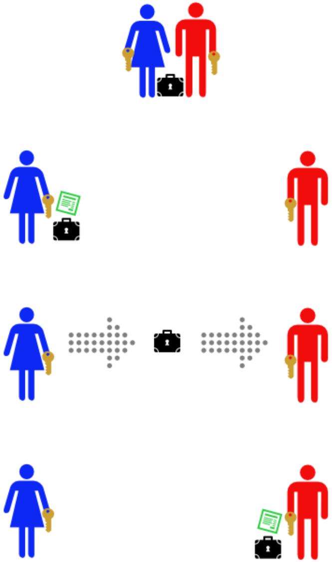


image credits: `https://wordtothewise.com/`

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say ‘Hello’ to Bob.

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say ‘Hello’ to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say ‘Hello’ to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say ‘Hello’ to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

m	b	x	a	z

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

m	b	x	a	z
12	1	23	0	25

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

	m	b	x	a	z
	12	1	23	0	25
−	5	23	12	15	11

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

	m	b	x	a	z
	12	1	23	0	25
−	5	23	12	15	11
	7	-22	11	- 15	14

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say ‘Hello’ to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

	m	b	x	a	z
	12	1	23	0	25
−	5	23	12	15	11
	7	-22	11	- 15	14
(26)	7	4	11	11	14

One-time pad

Alice and Bob both have access to the same (secret) list of random numbers.

$$5, 23, 12, 15, 11, 9, 3, 4, 6, 24, 9, 3, 6, 5, 15, 7, 24, \ldots$$

Alice wants to say 'Hello' to Bob.

Alice

	h	e	l	l	o
	7	4	11	11	14
+	5	23	12	15	11
	12	27	23	26	25
(26)	12	1	23	0	25
	m	b	x	a	z

Bob

	m	b	x	a	z
	12	1	23	0	25
−	5	23	12	15	11
	7	-22	11	- 15	14
(26)	7	4	11	11	14
	h	e	l	l	o

Random numbers

Problem. Need random numbers! How can we generate them?

Random numbers

Problem. Need random numbers! How can we generate them?

- Truly random numbers can only come from a physical process.

Random numbers

Problem. Need random numbers! How can we generate them?

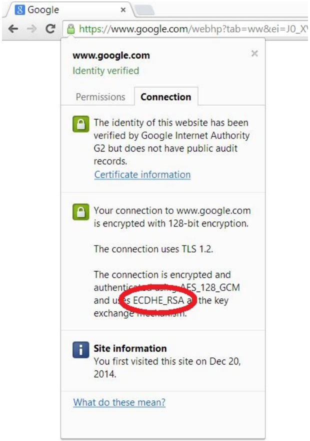
- Truly random numbers can only come from a physical process.
- We can generate numbers that appear random from a *recipe* using a computational device. These are called *pseudo-random numbers*.

Problem. Need random numbers! How can we generate them?

- Truly random numbers can only come from a physical process.
- We can generate numbers that appear random from a *recipe* using a computational device. These are called *pseudo-random numbers*.

One method comes from the theory of elliptic curves, which are recently very common in cryptography.

Google Chrome:



Key exchange: ECDHE_RSA

EC = Elliptic Curve

Elliptic curves

Elliptic curves are a special kind of cubic curves on the plane.

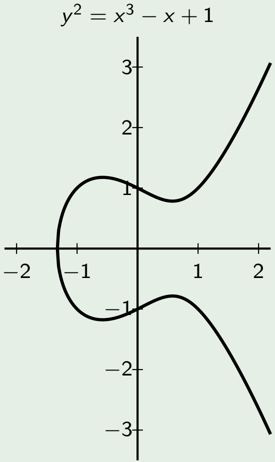
Definition

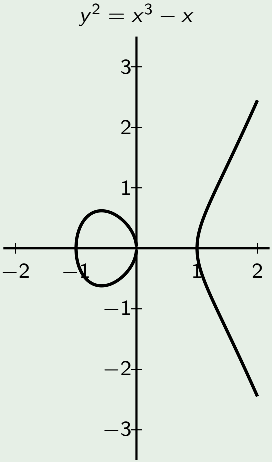
An *elliptic curve* over $\mathbb{R}$ is the set of solution $(x, y) \in \mathbb{R}^2$ of

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

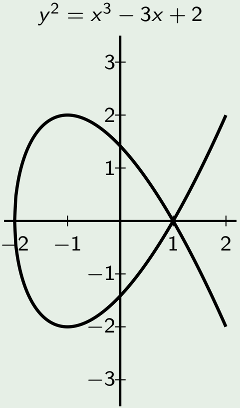
for $a, b \in \mathbb{R}$ such that $27b^2 + 4a^3 \neq 0$, together with a point O called the *point at infinity*.

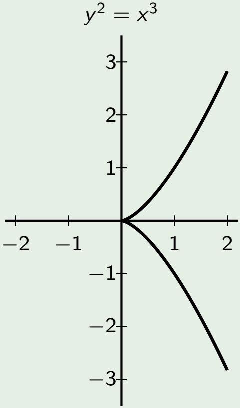
Examples





Non-examples

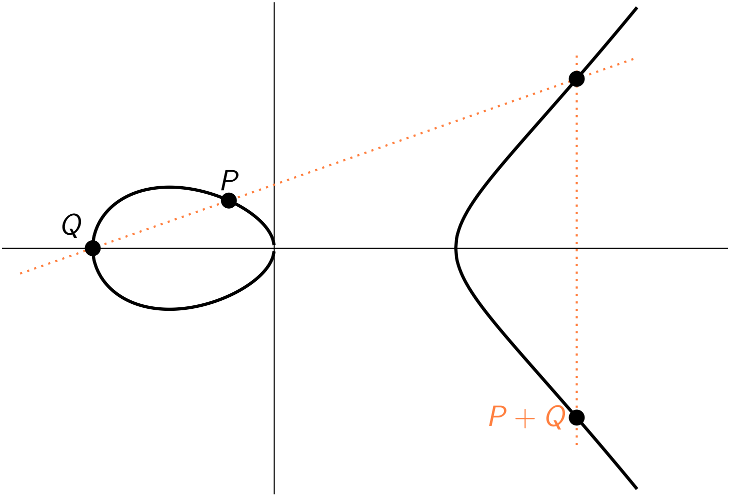




In the first one, we cannot define a tangent at the point $(1, 0)$. In the second one we cannot define a tangent at $(0, 0)$.

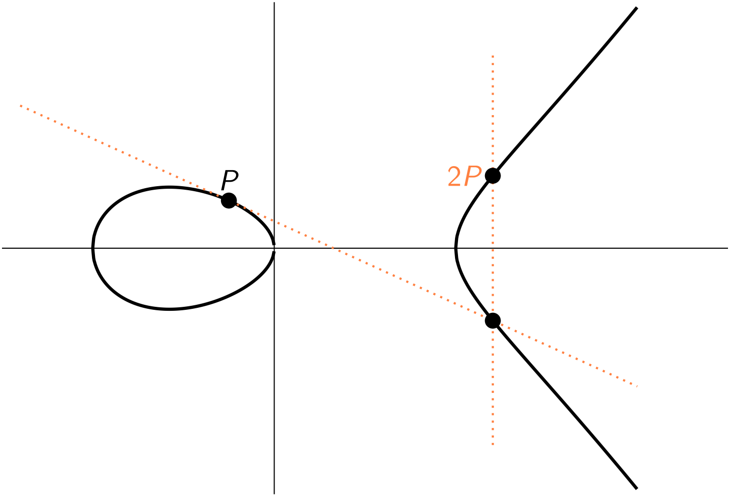
Addition on elliptic curves

Why are they so useful? You can define *addition* on them!



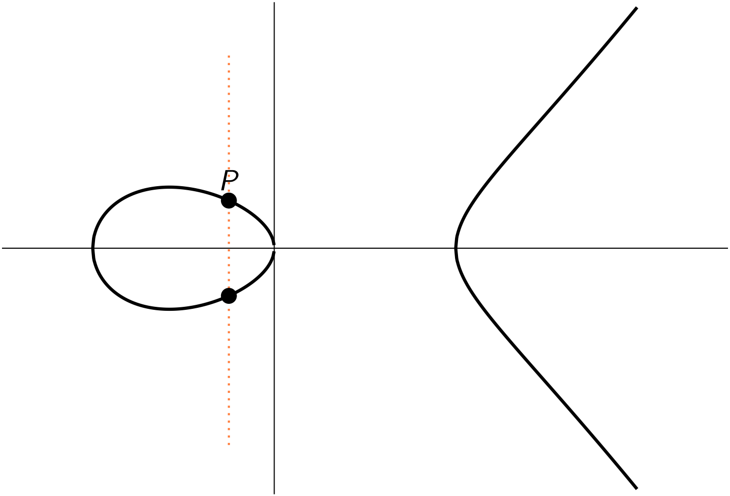
Addition on elliptic curves

Why are they so useful? You can define *addition* on them!



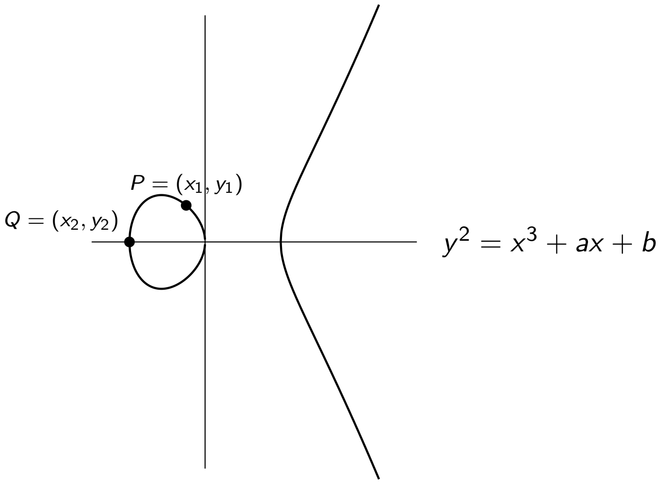
Addition on elliptic curves

Why are they so useful? You can define *addition* on them!

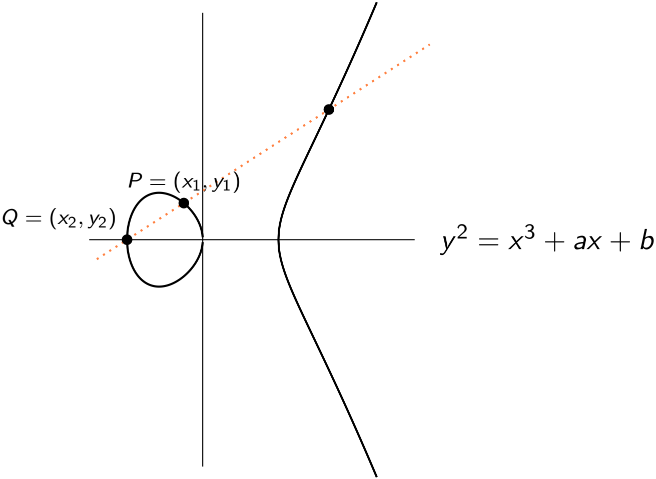


Addition on elliptic curves

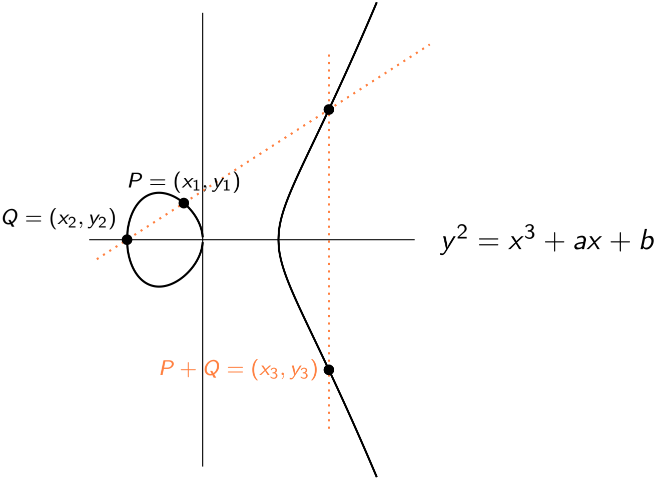
Problem. The definition is geometric. We need formulas!



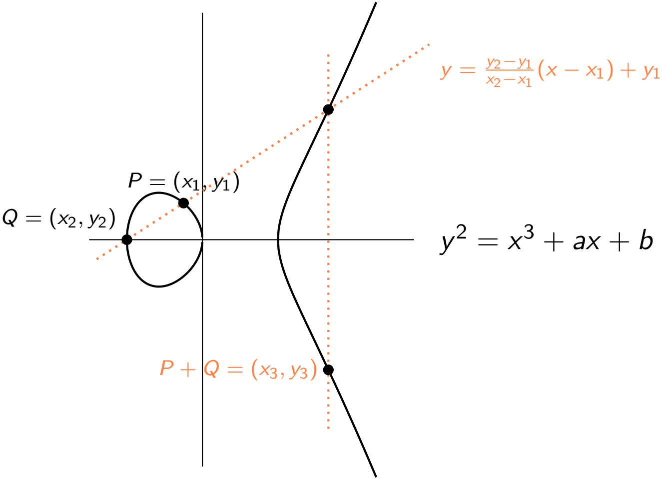
Problem. The definition is geometric. We need formulas!



Problem. The definition is geometric. We need formulas!

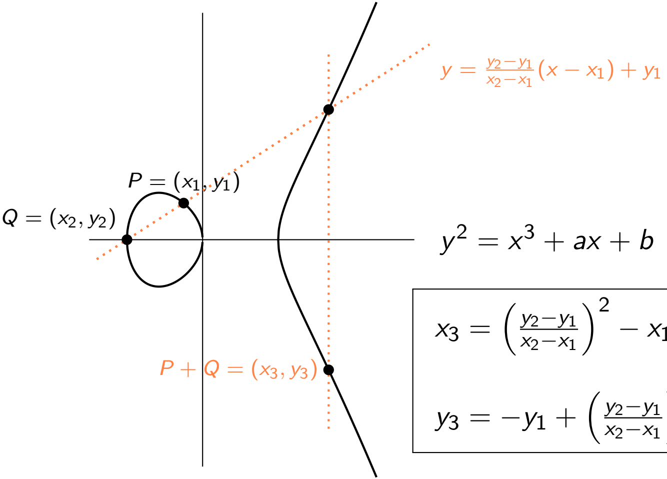


Problem. The definition is geometric. We need formulas!



Addition on elliptic curves

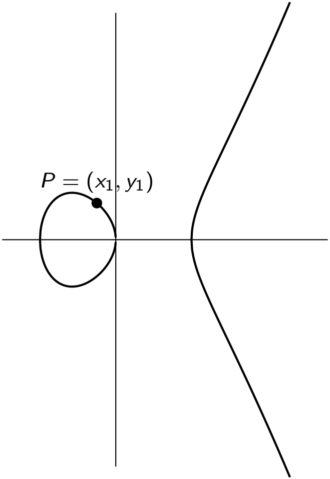
Problem. The definition is geometric. We need formulas!



$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

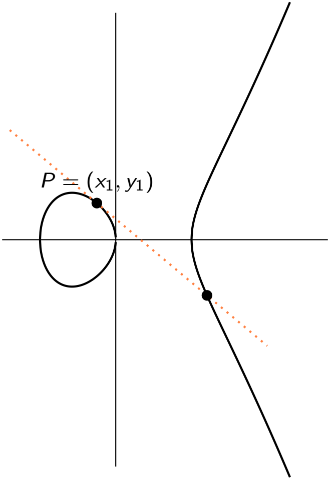
$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

Problem. The definition is geometric. We need formulas!



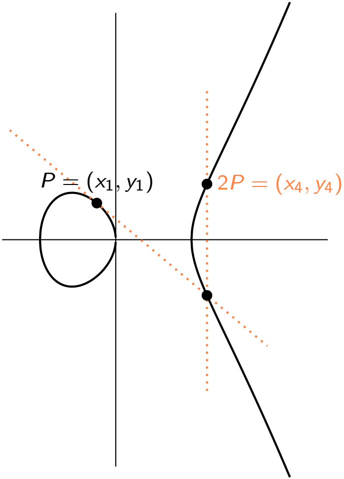
$$y^2 = x^3 + ax + b$$

Problem. The definition is geometric. We need formulas!



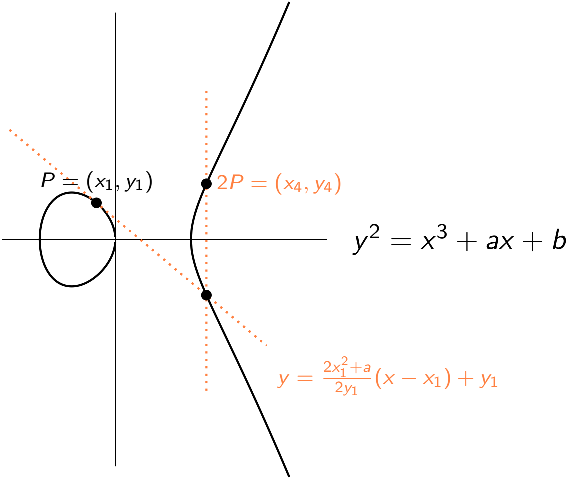
$$y^2 = x^3 + ax + b$$

Problem. The definition is geometric. We need formulas!



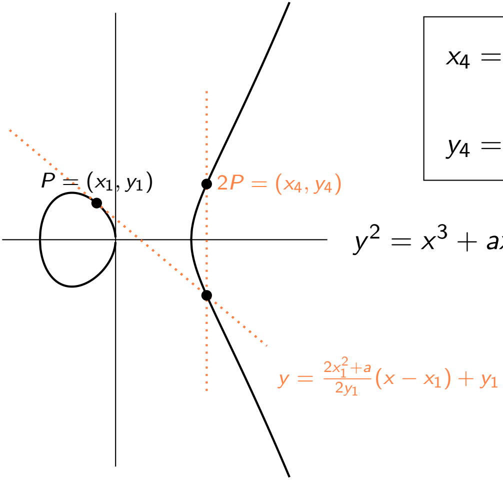
$$y^2 = x^3 + ax + b$$

Problem. The definition is geometric. We need formulas!



Addition on elliptic curves

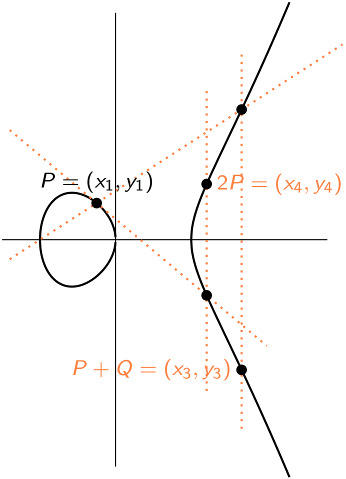
Problem. The definition is geometric. We need formulas!



$$x_4 = \left(\frac{3x^2+a}{2y_1}\right)^2 - 2x_1$$

$$y_4 = -y_1 + \left(\frac{3x^2+a}{2y_1}\right)(x_1 - x_4)$$

Problem. The definition is geometric. We need formulas!



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

$$x_4 = \left(\frac{3x^2+a}{2y_1}\right)^2 - 2x_1$$

$$y_4 = -y_1 + \left(\frac{3x^2+a}{2y_1}\right)(x_1 - x_3)$$

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3)$$

Elliptic curves

Computers are good with finite objects.

Computers are good with finite objects.

We can make elliptic curves finite by reducing them modulo a prime number p:

$$E[\mathbb{F}_p] = \{(x,y) \mid y^2 \equiv x^3 + ax + b \mod p\} \cup \{O\}$$

where $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ and $27b^2 + 4a^3 \not\equiv 0 \mod p$.

Computers are good with finite objects.

We can make elliptic curves finite by reducing them modulo a prime number p:

$$E[\mathbb{F}_p] = \{(x, y) \mid y^2 \equiv x^3 + ax + b \mod p\} \cup \{O\}$$

where $a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$ and $27b^2 + 4a^3 \not\equiv 0 \mod p$. The addition formulas also reduce modulo p, because they only use $+$, $-$, $\times$, $\div$. We can do all of these in $\mathbb{F}_p$.

Pseudo-random number generation

Public:

- E elliptic curve
- p prime number
- $P, Q \in E[\mathbb{F}_p]$

Pseudo-random number generation

Public:

- E elliptic curve
- p prime number
- $P, Q \in E[\mathbb{F}_p]$

Secret:

- $s \in \mathbb{N}$ seed (*internal state* of the algorithm).

Pseudo-random number generation

Public:

- E elliptic curve
- p prime number
- $P, Q \in E[\mathbb{F}_p]$

Secret:

- $s \in \mathbb{N}$ seed (*internal state* of the algorithm).

Algorithm

1. Let r be the x-coordinate of $sP = \underbrace{P + P + \ldots + P}_{s \text{ times}}$.

Pseudo-random number generation

Public:

- E elliptic curve
- p prime number
- $P, Q \in E[\mathbb{F}_p]$

Secret:

- $s \in \mathbb{N}$ seed (*internal state* of the algorithm).

Algorithm

1. Let r be the x-coordinate of $sP = \underbrace{P + P + \ldots + P}_{s \text{ times}}$.
2. Let t be the x-coordinate of $rQ = \underbrace{Q + Q + \ldots + Q}_{r \text{ times}}$. Then t is the random number.

Pseudo-random number generation

Public:

- E elliptic curve
- p prime number
- $P, Q \in E[\mathbb{F}_p]$

Secret:

- $s \in \mathbb{N}$ seed (*internal state* of the algorithm).

Algorithm

1. Let r be the x-coordinate of $sP = \underbrace{P + P + \ldots + P}_{s \text{ times}}$.
2. Let t be the x-coordinate of $rQ = \underbrace{Q + Q + \ldots + Q}_{r \text{ times}}$. Then t is the random number.
3. Let s' be the x-coordinate of $rP = \underbrace{P + P + \ldots + P}_{r \text{ times}}$. This is the new *internal state*.

Pseudo-random number generation

This was one of the four official pseudo-random number generators recommended by the National Institute of Standards and Technology (NIST).

NIST specifies this data: E, p, $n = \#E[\mathbb{F}_p]$, P, Q.

Pseudo-random number generation

This was one of the four official pseudo-random number generators recommended by the National Institute of Standards and Technology (NIST).
NIST specifies this data: E, p, $n = \#E[\mathbb{F}_p]$, P, Q.

There is a back door to this pseudo-random number generator; that is, a way to find the hidden state s and predict the "*random*" numbers.

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

Proof.

There are two possible points A with x-coordinate t — one of them is rQ and the other is $-rQ$.

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

Proof.

There are two possible points A with x-coordinate t — one of them is rQ and the other is $-rQ$. For both of them, we compute eA. For $A = rQ$ we get:

$$eA = e(rQ)$$

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

Proof.

There are two possible points A with x-coordinate t — one of them is rQ and the other is $-rQ$. For both of them, we compute eA. For $A = rQ$ we get:

$$eA = e(rQ) = r(eQ)$$

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

Proof.

There are two possible points A with x-coordinate t — one of them is rQ and the other is $-rQ$. For both of them, we compute eA. For $A = rQ$ we get:

$$eA = e(rQ) = r(eQ) = rP.$$

The back door

For all the curves E listed by NIST, the number of points of $E[\mathbb{F}_p]$ is prime. Since $E[\mathbb{F}_p]$ is a group of prime order, every element (except O) is a generator, so $P = eQ$ for some integer e.

Theorem

If we know e, we can extract the hidden state s' by observing the output t.

Proof.

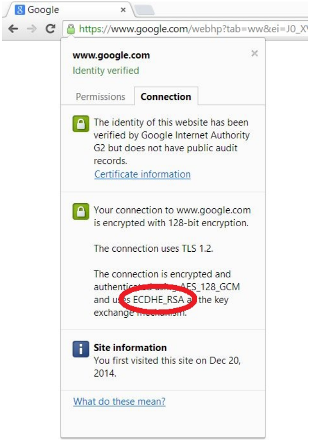
There are two possible points A with x-coordinate t — one of them is rQ and the other is $-rQ$. For both of them, we compute eA. For $A = rQ$ we get:

$$eA = e(rQ) = r(eQ) = rP.$$

But the new internal state s' is the x-coordinate of rP. □

Diffie–Hellman Key Exchange

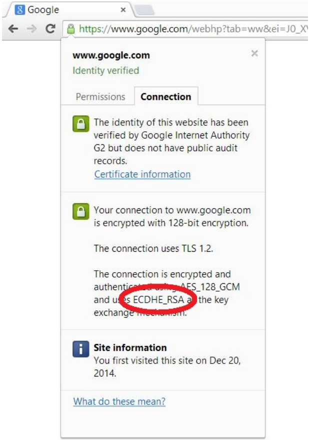
Let's go back to Google Chrome!



ECDHE = Elliptic Curve Diffie–Hellman key Exchange.

Diffie–Hellman Key Exchange

Let's go back to Google Chrome!



ECDHE = Elliptic Curve Diffie–Hellman key Exchange.

What is that? A commonly used well-known key exchange. Every cryptographer knows it.

It is based on the same idea as the back door!