Elliptic Curve Cryptography

christian wuthrich

May 6, 2010

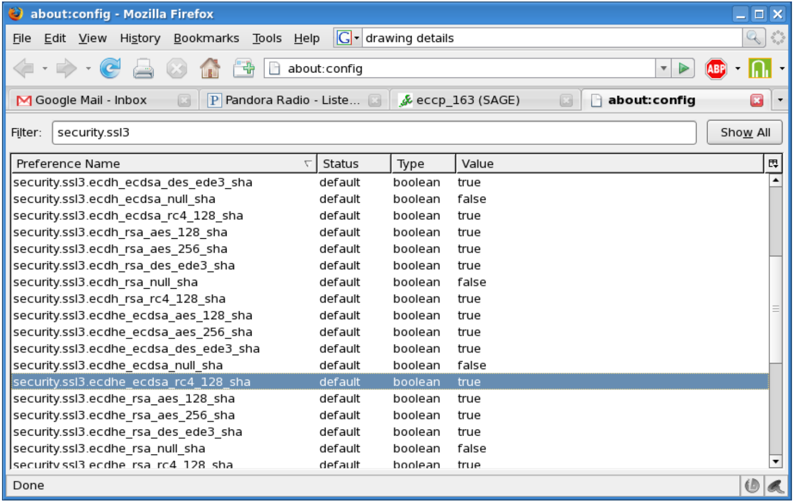
RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE

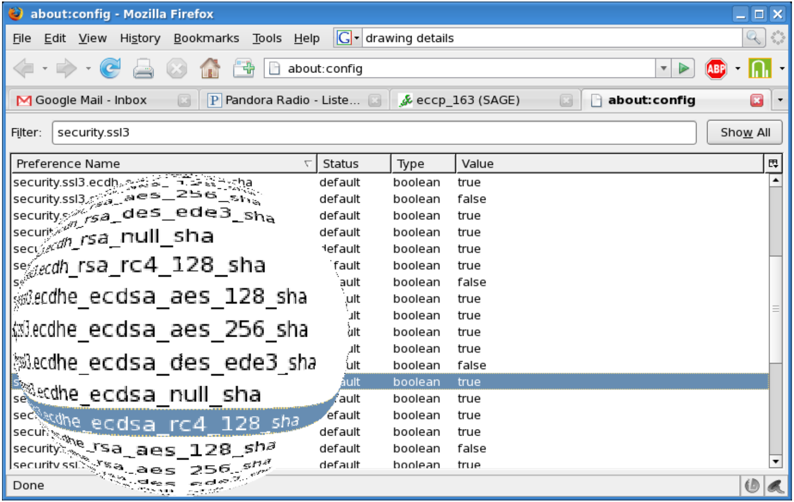
July 1999

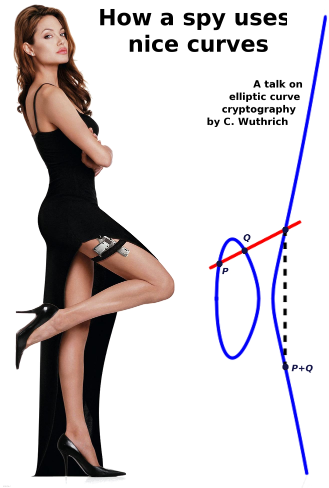
This collection of elliptic curves is recommended for Federal government use and contains choices of private key length and underlying fields.

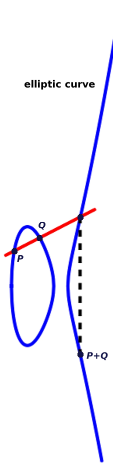
§1. Para… ter Choices

1.1 C… f Key Lengths


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
drawing details
about:config
Google Mail - Inbox
Pandora Radio - Liste...
eccp_163 (SAGE)
about:config
Filter: security.ssl3
Show All
Preference Name Status Type Value
security.ssl3.ecdh_ecdsa_des_ede3_sha default boolean true
security.ssl3.ecdh_ecdsa_null_sha default boolean false
security.ssl3.ecdh_ecdsa_rc4_128_sha default boolean true
security.ssl3.ecdh_rsa_aes_128_sha default boolean true
security.ssl3.ecdh_rsa_aes_256_sha default boolean true
security.ssl3.ecdh_rsa_des_ede3_sha default boolean true
security.ssl3.ecdh_rsa_null_sha default boolean false
security.ssl3.ecdh_rsa_rc4_128_sha default boolean true
security.ssl3.ecdhe_ecdsa_aes_128_sha default boolean true
security.ssl3.ecdhe_ecdsa_aes_256_sha default boolean true
security.ssl3.ecdhe_ecdsa_des_ede3_sha default boolean true
security.ssl3.ecdhe_ecdsa_null_sha default boolean false
security.ssl3.ecdhe_ecdsa_rc4_128_sha default boolean true
security.ssl3.ecdhe_rsa_aes_128_sha default boolean true
security.ssl3.ecdhe_rsa_aes_256_sha default boolean true
security.ssl3.ecdhe_rsa_des_ede3_sha default boolean true
security.ssl3.ecdhe_rsa_null_sha default boolean false
security.ssl3.ecdhe_rsa_rc4_128_sha default boolean true
Done


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
drawing details
about:config
Google Mail - Inbox
Pandora Radio - Liste...
eccp_163 (SAGE)
about:config
Filter: security.ssl3
Show All
Preference Name
Status
Type
Value
rsa_des_ede3_sha
rsa_null_sha
ecdh_rsa_rc4_128_sha
ecdhe_ecdsa_aes_128_sha
ecdhe_ecdsa_aes_256_sha
ecdhe_ecdsa_des_ede3_sha
ecdhe_ecdsa_null_sha
ecdhe_ecdsa_rc4_128_sha
rsa_aes_128_sha
rsa_aes_256_sha
default
boolean
true
false
Done


How a spy uses
nice curves
A talk on
elliptic curve
cryptography
by C. Wuthrich
Q
P
P+Q

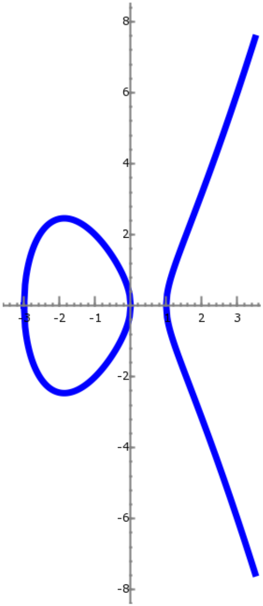

elliptic curve
Q
P
P+Q

An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

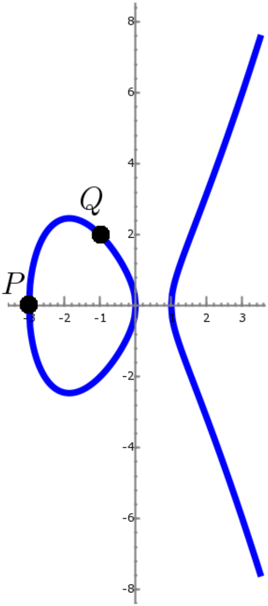


An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

$P = (-3, 0)$ and $Q = (-1, 2)$



An elliptic curve

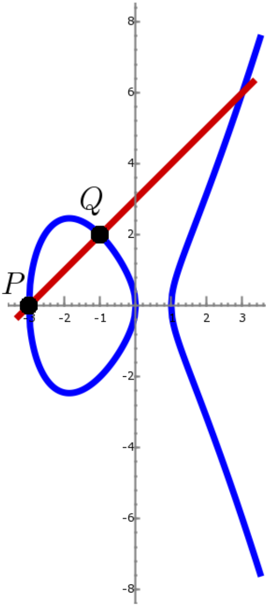
$$y^2 = x^3 + 2x^2 - 3x$$

Two points

$P = (-3, 0)$ and $Q = (-1, 2)$

are linked by a line

$$y = x + 3\,.$$



An elliptic curve

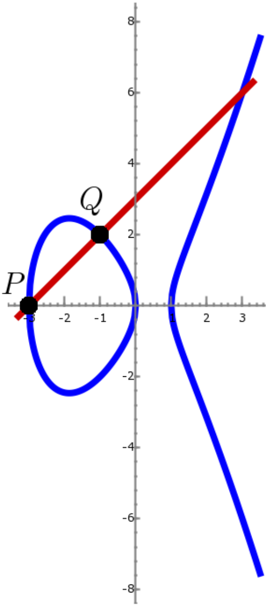
$$y^2 = x^3 + 2x^2 - 3x$$

Two points

$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2).$$

Putting into the elliptic curve

$$y^2 = (x+3)^2 = x^3 + 2x^2 - 3x$$



An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

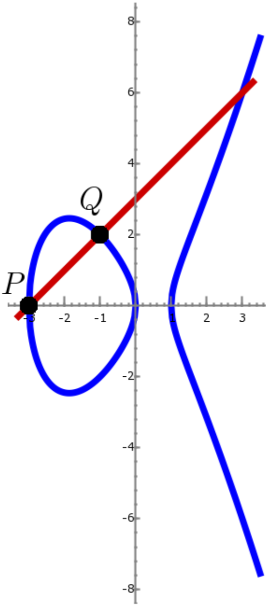
$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2).$$

Putting into the elliptic curve

$$y^2 = (x+3)^2 = x^3 + 2x^2 - 3x$$

yields

$$0 = x^3 + x^2 - 9x + 9.$$



An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

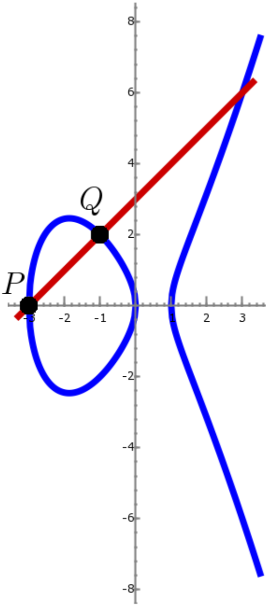
$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2).$$

Putting into the elliptic curve

$$y^2 = (x+3)^2 = x^3 + 2x^2 - 3x$$

yields

$$0 = (x+3) \cdot (x+1) \cdot (x-3).$$



An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

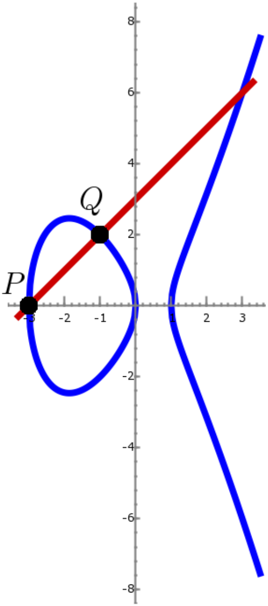
$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2).$$

Putting into the elliptic curve

$$y^2 = (x+3)^2 = x^3 + 2x^2 - 3x$$

yields

$$0 = (x+3) \cdot (x+1) \cdot {\color{red}(x-3)}.$$



An elliptic curve

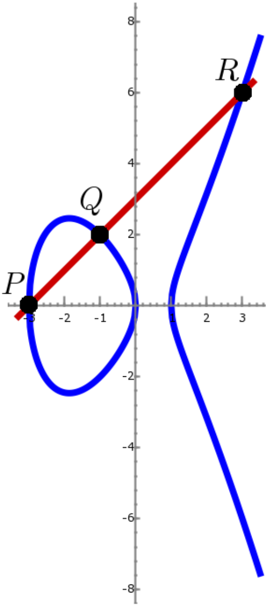
$$y^2 = x^3 + 2x^2 - 3x$$

Two points

$P = (-3, 0)$ and $Q = (-1, 2)$

give a new point

$$R = (3, 6)\,.$$



An elliptic curve

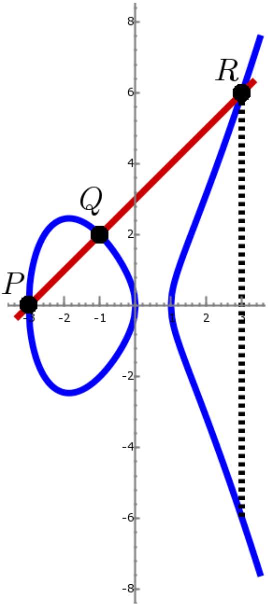
$$y^2 = x^3 + 2x^2 - 3x$$

Two points

$P = (-3, 0)$ and $Q = (-1, 2)$

give a new point

$$R = (3, 6)\,.$$



An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

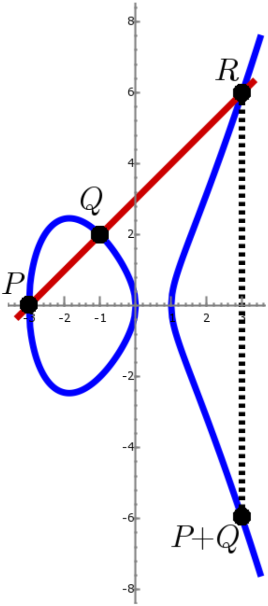
$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2)$$

give a new point

$$R = (3, 6) .$$

Put

$$P + Q := (3, -6) .$$



An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

Two points

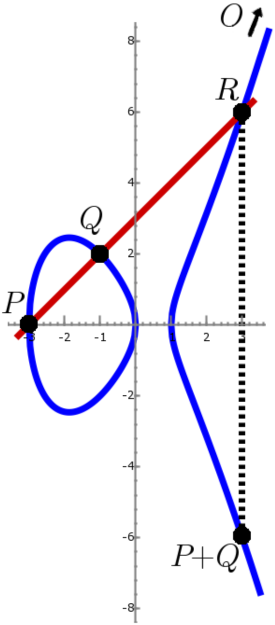
$$P = (-3, 0) \quad \text{and} \quad Q = (-1, 2)$$

give a new point

$$R = (3, 6)\,.$$

Put

$$P + Q := (3, -6)\,.$$

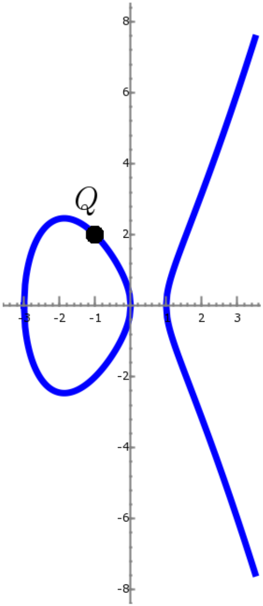


An elliptic curve

$$y^2 = x^3 + 2x^2 - 3x$$

One point

$$Q = (-1, 2)$$



An elliptic curve

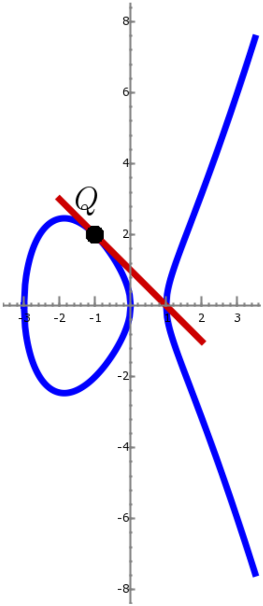
$$y^2 = x^3 + 2x^2 - 3x$$

One point

$$Q = (-1, 2)$$

has a tangent

$$y = -x + 1\,.$$



An elliptic curve

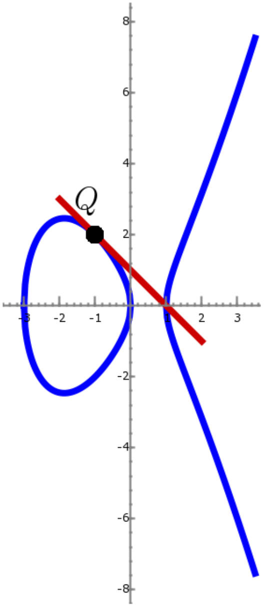
$$y^2 = x^3 + 2x^2 - 3x$$

One point

$$Q = (-1, 2)$$

Putting into the elliptic curve

$$y^2 = (-x+1)^2 = x^3 + 2x^2 - 3x$$
$$0 = x^3 + x^2 - x - 1\,.$$
$$0 = (x+1)\cdot(x+1)\cdot(x-1)\,.$$



An elliptic curve

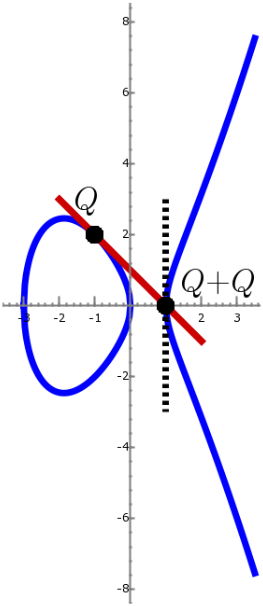
$$y^2 = x^3 + 2x^2 - 3x$$

One point

$$Q = (-1, 2)$$

gives a new point

$$2Q = Q + Q = (1, 0).$$



Let K be a field. An elliptic curve is an equation

$$y^2 = x^3 + Ax + B \qquad \text{with } A \text{ and } B \in K$$

Let K be a field. An elliptic curve is an equation

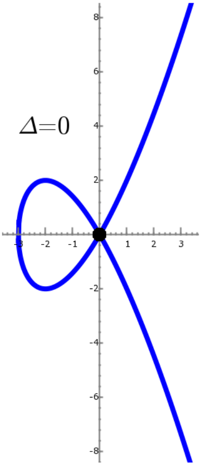
$$y^2 = x^3 + Ax + B \qquad \text{with } A \text{ and } B \in K$$

such that $\Delta = -16 \cdot (4A^3 + 27B^2) \neq 0$.

Let K be a field. An elliptic curve is an equation

$$y^2 = x^3 + Ax + B \qquad \text{with } A \text{ and } B \in K$$

such that $\Delta = -16 \cdot (4A^3 + 27B^2) \neq 0$.



Let K be a field. An elliptic curve is an equation

$$y^2 = x^3 + Ax + B \qquad \text{with } A \text{ and } B \in K$$

such that $\Delta = -16 \cdot (4A^3 + 27B^2) \neq 0$.

$$E(K) = \{O\} \cup \{ (x, y) \in K^2 \mid y^2 = x^3 + Ax + B \}$$

is an abelian group under the law $+$.

The sum of $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ is given by

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_{P+Q} = \lambda^2 - x_P - x_Q$$

$$y_{P+Q} = -\lambda \cdot x_{P+Q} - \frac{y_P\, x_Q - y_Q\, x_P}{x_Q - x_P}\,.$$

The sum of $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ is given by

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_{P+Q} = \lambda^2 - x_P - x_Q$$

$$y_{P+Q} = -\lambda \cdot x_{P+Q} - \frac{y_P\, x_Q - y_Q\, x_P}{x_Q - x_P}\,.$$

The rule for $2 \cdot P$ is a bit different

$$x_{2P} = \frac{x_P^4 - 2\,A\,x_P^2 - 4\,B\,x_P + A^2}{4\,y_P^2}\,.$$

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/_{13\mathbb{Z}} .$$

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/_{13\mathbb{Z}} \,.$$

We find the points

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}/_{13\mathbb{Z}} \,.$$

We find the points

$$(7,8) \qquad (8,8) \qquad (11,5) \qquad (11,8)$$

$$(8,5) \qquad (7,5) \qquad O$$

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/\!_{13\mathbb{Z}} \, .$$

We find the points

$$P = (7,8) \quad 2P = (8,8) \quad 3P = (11,5) \quad 4P = (11,8)$$
$$5P = (8,5) \qquad 6P = (7,5) \qquad 7P = O$$

$$E(K) \;\cong\; {}^{\mathbb{Z}}\!/\!_{7\mathbb{Z}}\, P \, .$$

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/_{13\mathbb{Z}}\,.$$

We find the points

$$P = (7,8) \quad 2P = (8,8) \quad 3P = (11,5) \quad 4P = (11,8)$$
$$5P = (8,5) \qquad 6P = (7,5) \qquad 7P = O$$

$$E(K) \;\cong\; {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}\, P\,.$$

In general, we have that

$$\#E\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right) \;\sim\; p\,.$$

Another curve

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/_{13\mathbb{Z}}\,.$$

We find the points

$$P = (7,8) \quad 2P = (8,8) \quad 3P = (11,5) \quad 4P = (11,8)$$
$$5P = (8,5) \qquad 6P = (7,5) \qquad 7P = O$$

$$E(K) \;\cong\; {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}\,P\,.$$

Or more precisely

Hasse–Weil

$$p + 1 - 2\sqrt{p} \;\leqslant\; \#E\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right) \;\leqslant\; p + 1 + 2\sqrt{p}$$

Curve sepc160k1

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}\!/\!_{p\mathbb{Z}} \qquad \text{with}$$

$$p = 2^{160} - 2^{32} - 21389$$

$$= 1461501637330902918203684832716283019651637554291.$$

Curve sepc160k1

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}/_{p\mathbb{Z}} \qquad \text{with}$$
$$p = 2^{160} - 2^{32} - 21389$$
$$= 1461501637330902918203684832716283019651637554291.$$

Here we have

$$\#E(K) = 1461501637330902918203686915170869725397159163571$$
$$= p + 1 + 2082454586705745521609279$$

Curve sepc160k1

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}/_{p\mathbb{Z}} \qquad \text{with}$$
$$p = 2^{160} - 2^{32} - 21389$$
$$= 1461501637330902918203684832716283019651637554291.$$

Here we have

$$\begin{aligned} \#E(K) &= 1461501637330902918203686915170869725397159163571 \\ &= p \; + \; 1 \; + \; 2082454586705745521609279 \end{aligned}$$

This number is a prime, too. So $E(K)$ is cyclic.

Curve sepc160k1

$$y^2 = x^3 + 7 \quad \text{over} \quad \mathbb{Z}/_{p\mathbb{Z}} \quad \text{with}$$
$$p = 2^{160} - 2^{32} - 21389$$
$$= 1461501637330902918203684832716283019651637554291.$$

Here we have

$$\begin{aligned}\#E(K) &= 1461501637330902918203686915170869725397159163571\\ &= p + 1 + 2082454586705745521609279\end{aligned}$$

This number is a prime, too. So $E(K)$ is cyclic.
Any random point P is a generator, like

Curve sepc160k1

$$y^2 = x^3 + 7 \qquad \text{over} \qquad {}^{\mathbb{Z}}/_{p\mathbb{Z}} \qquad \text{with}$$
$$p = 2^{160} - 2^{32} - 21389$$
$$= 1461501637330902918203684832716283019651637554291.$$

Here we have

$$\#E(K) = 1461501637330902918203686915170869725397159163571$$
$$= p + 1 + 2082454586705745521609279$$

This number is a prime, too. So $E(K)$ is cyclic.
Any random point P is a generator, like

$$x = 3$$
$$y = 711760731743902376321964521567630871968071244 40.$$

Curve sepc160k1

$$y^2 = x^3 + 7 \quad \text{over} \quad {}^{\mathbb{Z}}/_{p\mathbb{Z}} \quad \text{with}$$

$$p = 2^{160} - 2^{32} - 21389$$

$$= 1461501637330902918203684832716283019651637554291.$$

Here we have

$$\#E(K) = 1461501637330902918203686915170869725397159163571$$
$$= p + 1 + 2082454586705745521609279$$

This number is a prime, too. So $E(K)$ is cyclic.
Any random point P is a generator, like

$$x = 1113129110347110584529936623496597364692506205616$$
$$y = 1091969504653372982238646049713444006222837815293\,.$$

Alice

Alice

Alice would like to talk to Bob.

Alice would like to talk to

Bob.

Alice would like to talk to Bob.

Alice wants to send I LOVEYOUBOB to Bob.

Alice would like to talk to Bob.

Alice wants to send I LOVEYOUBOB to Bob.
She uses the secret key $K =$ABRACADABRA.

Alice would like to talk to Bob.

Alice wants to send I LOVEYOUBOB to Bob.
She uses the secret key $K =$ABRACADABRA.
The encrypted message is JMFWHZSVDFC.

Alice would like to talk to Bob.

Alice wants to send I L O V EYOUBOB to Bob.
She uses the secret key K =A B R A CADABRA.
The encrypted message is JMFWHZSVDFC.

How does Bob get K ?

They agree on

They agree on

- A prime p.

They agree on

- A prime p.
- An elliptic curve E over ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.

They agree on

- A prime p.
- An elliptic curve E over ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.
- A point P in $E\left({}^{\mathbb{Z}}/_{p\mathbb{Z}}\right)$.

They agree on

- A prime p.
- An elliptic curve E over ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$.
- A point P in $E\left({}^{\mathbb{Z}}/_{p\mathbb{Z}}\right)$.

The triple (p, E, P) is publically known.

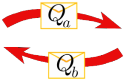
Fixed : (p, E, P)

Fixed : (p, E, P)

Fixed : (p, E, P)

- Chooses $0 \leqslant a < N = \#E(K)$.
- Chooses $0 \leqslant b < N$.

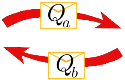
Fixed : (p, E, P)



- Chooses $0 \leqslant \color{red}{a} < N = \#E(K)$.
- Sends $Q_a = a \cdot P$.

- Chooses $0 \leqslant \color{red}{b} < N$.
- Sends $Q_b = b \cdot P$.

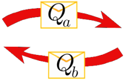
Fixed : (p, E, P)



- Chooses $0 \leqslant {\color{red}a} < N = \#E(K)$.
- Sends $Q_a = a \cdot P$.
- Computes $a \cdot Q_b$.

- Chooses $0 \leqslant {\color{red}b} < N$.
- Sends $Q_b = b \cdot P$.
- Computes $b \cdot Q_a$.

Fixed : (p, E, P)



- Chooses $0 \leqslant \color{red}{a} < N = \#E(K)$.
- Sends $Q_a = a \cdot P$.
- Computes $a \cdot Q_b$.

- Chooses $0 \leqslant \color{red}{b} < N$.
- Sends $Q_b = b \cdot P$.
- Computes $b \cdot Q_a$.

They both have the same

$$K = a \cdot Q_b = a \cdot (b \cdot P) = (ab) \cdot P = b \cdot (a \cdot P) = b \cdot Q_a$$

Eve wants to listen to the conversation.

Eve wants to listen to the conversation.

She knows

$$p \qquad E \qquad P \qquad Q_a = a\,P \qquad Q_b = b\,P$$

Eve wants to listen to the conversation.

She knows

$$p \qquad E \qquad P \qquad Q_a = a\,P \qquad Q_b = b\,P$$

but she wants to know $K = a\,b\,P$.

Eve wants to listen to the conversation.

She knows

$$p \qquad E \qquad P \qquad Q_a = a\,P \qquad Q_b = b\,P$$

but she wants to know $K = a\,b\,P$.

Discrete Logarithm

Given $P, Q \in E(K)$, find m such that $Q = m\,P$.

Eve wants to listen to the conversation.

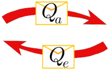
She knows

$$p \qquad E \qquad P \qquad Q_a = a\,P \qquad Q_b = b\,P$$

but she wants to know $K = a\,b\,P$.

Discrete Logarithm

Given $P, Q \in E(K)$, find m such that $Q = m\,P$.


- Alice creates a key with Eve, believing that she is talking to Bob.

- Alice creates a key with Eve, believing that she is talking to Bob.
- Bob creates a key with Eve, believing that he is talking to Alice.

- Alice creates a key with Eve, believing that she is talking to Bob.
- Bob creates a key with Eve, believing that he is talking to Alice.

Alice should sign her letter.

- Chooses a signature s

- Chooses a signature s
- Chooses $0 \leqslant k < N$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(kP) \bmod N$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(kP) \bmod N$.
- $t = (s + ar) \cdot k^{-1} \bmod N$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(k P) \bmod N$.
- $t = (s + a r) \cdot k^{-1} \bmod N$.
- Sends (s, r, t) to Bob.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(k\,P) \bmod N$.
- $t = (s + a\,r) \cdot k^{-1} \bmod N$.
- Sends (s, r, t) to Bob.

- $u = s \cdot t^{-1} \bmod N$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(kP) \bmod N$.
- $t = (s + ar) \cdot k^{-1} \bmod N$.
- Sends (s, r, t) to Bob.

- $u = s \cdot t^{-1} \bmod N$.
- $v = r \cdot t^{-1} \bmod N$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(k\,P) \bmod N$.
- $t = (s + a\,r) \cdot k^{-1} \bmod N$.
- Sends (s, r, t) to Bob.

- $u = s \cdot t^{-1} \bmod N$.
- $v = r \cdot t^{-1} \bmod N$.
- $R = u \cdot P + v \cdot Q_a$.

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(k\,P) \mod N$.
- $t = (s + a\,r) \cdot k^{-1} \mod N$.
- Sends (s, r, t) to Bob.

- $u = s \cdot t^{-1} \mod N$.
- $v = r \cdot t^{-1} \mod N$.
- $R = u \cdot P + v \cdot Q_a$.
- Signature is ok if $x(R) \equiv r \pmod N$

- Chooses a signature s
- Chooses $0 \leqslant k < N$.
- $r = x(kP) \bmod N$.
- $t = (s + ar) \cdot k^{-1} \bmod N$.
- Sends (s, r, t) to Bob.

- $u = s \cdot t^{-1} \bmod N$.
- $v = r \cdot t^{-1} \bmod N$.
- $R = u \cdot P + v \cdot Q_a$.
- Signature is ok if $x(R) \equiv r \pmod N$

$$R = uP + vQ_a = st^{-1}P + rt^{-1}aP = (s + ra) \cdot t^{-1} \cdot P = kP$$

Easy

Find a large prime

Easy

Find a large prime

Easy

Count the number of points in $E(K)$.

Easy

Find a large prime

Easy

Count the number of points in $E(K)$.

Hard : Discrete Logarithm

Given $P, Q \in E(K)$, find m such that $Q = mP$.

Easy

Find a large prime

Easy

Count the number of points in $E(K)$.

Hard : Discrete Logarithm

Given $P, Q \in E(K)$, find m such that $Q = mP$.

RSA versus ECC

RSA versus ECC

Elliptic Curve Cryptography is much better.

RSA versus ECC

Elliptic Curve Cryptography is much better.

ECC	RSA	speed	size
160	1024	2.4	6.4
192	1536	7.1	8
224	2048	11	9.1

RSA versus ECC

Elliptic Curve Cryptography is much better.

ECC	RSA	speed	size
160	1024	2.4	6.4
192	1536	7.1	8
224	2048	11	9.1

SOURCE: SUN MICROSYSTEMS

Current use

Current use

- National Security Agency recommends it

Current use

- National Security Agency recommends it
- Sun Microsystems (java)

Current use

- National Security Agency recommends it
- Sun Microsystems (java)
- SSL / TLS

Current use

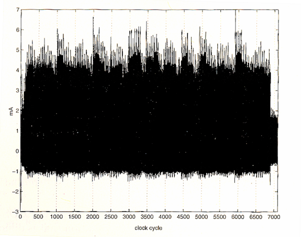
- National Security Agency recommends it
- Sun Microsystems (java)
- SSL / TLS
- Biometric passport

Current use

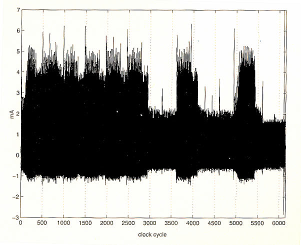
- National Security Agency recommends it
- Sun Microsystems (java)
- SSL / TLS
- Biometric passport
- Wii

Side-attacks

Reading the power-consumption on a smart-card



$P + Q$



$2 \cdot P$

Certicom challenge

Bit-size	Machine days	prize	state
79	146	a book	Dec. ’97
89	4360	a book	Jan. ’98
97	71982	5000 $	Mar. ’98
109	$9 \cdot 10^7$	10000 $	Nov. ’02
131	$2.3 \cdot 10^{10}$	20000 $	open
163	$2.3 \cdot 10^{15}$	30000 $	
191	$4.8 \cdot 10^{19}$	40000 $	
238	$1.4 \cdot 10^{27}$	50000 $	
353	$3.7 \cdot 10^{45}$	100000 $	

SOURCE: WWW.CERTICOM.COM

THE END