Week 8: Elliptic Curve Cryptography

Jay Daigle

Occidental College

October 17, 2019

$\mathbb{F}_{13}$

$\mathbb{F}_{13}$

$$1^2 \equiv 1 \qquad 2^2 \equiv 4 \qquad 3^3 \equiv 9 \qquad 4^3 \equiv 3 \qquad 5^2 \equiv 12 \qquad 6^2 \equiv 10$$

$$7^2 \equiv 10 \qquad 8^2 \equiv 12 \qquad 9^2 \equiv 3 \qquad 10^2 \equiv 9 \qquad 11^2 \equiv 4 \qquad 12^2 \equiv 1$$

$\mathbb{F}_{13}$

$$
\begin{array}{cccccc}
1^2 \equiv 1 & 2^2 \equiv 4 & 3^3 \equiv 9 & 4^3 \equiv 3 & 5^2 \equiv 12 & 6^2 \equiv 10 \\
7^2 \equiv 10 & 8^2 \equiv 12 & 9^2 \equiv 3 & 10^2 \equiv 9 & 11^2 \equiv 4 & 12^2 \equiv 1
\end{array}
$$

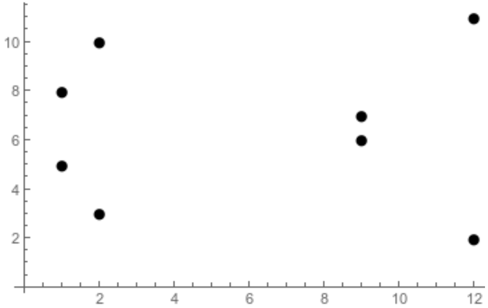
$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$

$\mathbb{F}_{13}$

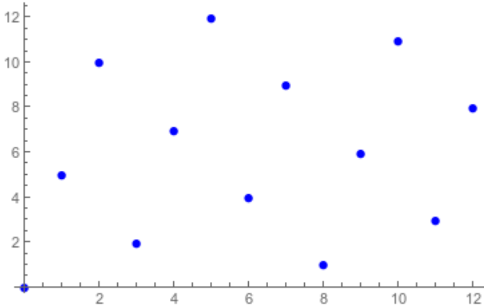
$$
\begin{array}{cccccc}
1^2 \equiv 1 & 2^2 \equiv 4 & 3^3 \equiv 9 & 4^3 \equiv 3 & 5^2 \equiv 12 & 6^2 \equiv 10 \\
7^2 \equiv 10 & 8^2 \equiv 12 & 9^2 \equiv 3 & 10^2 \equiv 9 & 11^2 \equiv 4 & 12^2 \equiv 1
\end{array}
$$

$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$

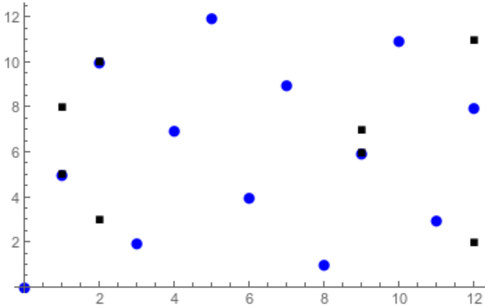
$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$



$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$



The line $y = 5x$ over $\mathbb{F}_{13}$



$$y^2 = x^3 + 3x + 8 \text{ and } y = 5x$$

Proposition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $E(\mathbb{Q})$. Then:

Proposition

Let $E : y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{Q}$*, and let* $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$ *be points on* $E(\mathbb{Q})$*. Then:*

1. *If* $y_1 \equiv -y_2 \mod p$ *then* $P \oplus Q = \mathcal{O}$*.*

Proposition

Let $E : y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{Q}$*, and let* $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$ *be points on* $E(\mathbb{Q})$*. Then:*

1. *If* $y_1 \equiv -y_2 \mod p$ *then* $P \oplus Q = \mathcal{O}$*.*
2. *If* $P_1 = P_2$*, then define* $\lambda = \frac{3x_1^2 + A}{2y_1}$*. Set*

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Then $P \oplus Q = (x_3, y_3)$*.*

Proposition

Let $E : y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{Q}$*, and let* $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$ *be points on* $E(\mathbb{Q})$*. Then:*

1. *If* $y_1 \equiv -y_2 \mod p$ *then* $P \oplus Q = \mathcal{O}$*.*
2. *If* $P_1 = P_2$*, then define* $\lambda = \frac{3x_1^2 + A}{2y_1}$*. Set*

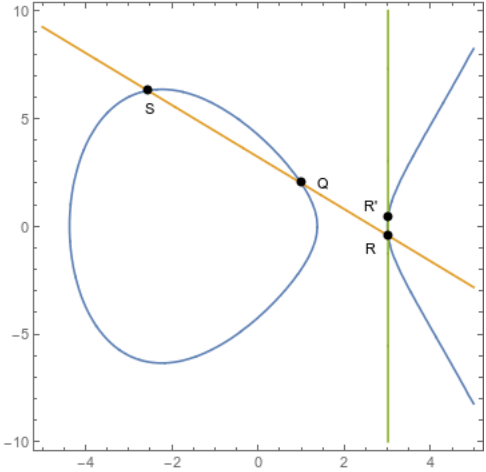
$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

   Then $P \oplus Q = (x_3, y_3)$*.*

3. *If* $P_1 \neq P_2$*, then define* $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$*. Then as before, set*

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

   Then $P \oplus Q = (x_3, y_3)$*.*


10
5
0
−5
−10
−4
−2
0
2
4
S
Q
R'
R

Calculations

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ *such that* $Q = nP$.

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ such that $Q = nP$. Write $n = \log_P(Q)$ for the elliptic discrete logarithm of Q with respect to P (on the curve $E/_p$) .

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ such that $Q = nP$. Write $n = \log_P(Q)$ for the elliptic discrete logarithm of Q with respect to P (on the curve $E/_p$) .

Double and Add

Want to compute nP for $P \in E(_p)$. Let $k = \log_2(n)$. Then:

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ such that $Q = nP$. Write $n = \log_P(Q)$ for the elliptic discrete logarithm of Q with respect to P (on the curve $E/_p$) .

Double and Add

Want to compute nP for $P \in E(_p)$. Let $k = \log_2(n)$. Then:

1. Compute $2^k P$ for $2^k \leq a$. That is, compute $g, g^2, g^4, g^8, \ldots, g^{2^k}$.

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ such that $Q = nP$. Write $n = \log_P(Q)$ for the elliptic discrete logarithm of Q with respect to P (on the curve $E/_p$) .

Double and Add

Want to compute nP for $P \in E(_p)$. Let $k = \log_2(n)$. Then:

1. Compute $2^k P$ for $2^k \leq a$. That is, compute $g, g^2, g^4, g^8, \ldots, g^{2^k}$.
2. Now express n in binary. That is, write $n = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_k 2^k$, where $c_i \in \{0, 1\}$.

Calculations

Definition

The elliptic curve discrete logarithm problem: find $n \in$ such that $Q = nP$. Write $n = \log_P(Q)$ for the elliptic discrete logarithm of Q with respect to P (on the curve $E/_p$) .

Double and Add

Want to compute nP for $P \in E(_p)$. Let $k = \log_2(n)$. Then:

1. Compute $2^k P$ for $2^k \leq a$. That is, compute $g, g^2, g^4, g^8, \ldots, g^{2^k}$.
2. Now express n in binary. That is, write $n = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_k 2^k$, where $c_i \in \{0, 1\}$.
3. Now we can compute

$$nP = (c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_k 2^k)P = c_0 P \oplus c_1 2P \oplus c_2 4P \oplus \cdots \oplus$$

Elliptic Curve Diffie-Hellman

Elliptic Curve Diffie-Hellman

Alice and Bob wish to exchange a key. They follow the following steps:

Elliptic Curve Diffie-Hellman

Alice and Bob wish to exchange a key. They follow the following steps:

1. A public party chooses a large prime p, and an elliptic curve E over $_p$, and a point $P \in E(_p)$.

Elliptic Curve Diffie-Hellman

Alice and Bob wish to exchange a key. They follow the following steps:

1. A public party chooses a large prime p, and an elliptic curve E over $_p$, and a point $P \in E(_p)$.
2. Alice chooses a secret integer n_A, and Bob chooses a secret integer n_B. Neither party reveals this integer to anyone.

Elliptic Curve Diffie-Hellman

Alice and Bob wish to exchange a key. They follow the following steps:

1. A public party chooses a large prime p, and an elliptic curve E over $_p$, and a point $P \in E(_p)$.
2. Alice chooses a secret integer n_A, and Bob chooses a secret integer n_B. Neither party reveals this integer to anyone.
3. Alice computes $Q_A = n_A P$ and Bob computes $Q_B = n_B P$. They (publicly) exchange these values with each other.

Elliptic Curve Diffie-Hellman

Alice and Bob wish to exchange a key. They follow the following steps:

1. A public party chooses a large prime p, and an elliptic curve E over $_p$, and a point $P \in E(_p)$.
2. Alice chooses a secret integer n_A, and Bob chooses a secret integer n_B. Neither party reveals this integer to anyone.
3. Alice computes $Q_A = n_A P$ and Bob computes $Q_B = n_B P$. They (publicly) exchange these values with each other.
4. Now Alice computes $n_A Q_B$ and Bob computes $n_B Q_A$.

Elliptic Curve ElGamal

Elliptic Curve ElGamal

Alice generates a key:

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over $_p$, and a point $P \in E(_p)$ of large order.
2. Alice chooses a private key n_A.

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Bob sends a message $M \in E({}_p)$:

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Bob sends a message $M \in E({}_p)$:

1. Bob generates a random ephemeral key k.

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Bob sends a message $M \in E({}_p)$:

1. Bob generates a random ephemeral key k.
2. Bob computes $C_1 = kP \in E({}_p), C_2 = M + kQ_A \in E({}_p)$. Bob transmits the pair of points (C_1, C_2) to Alice.

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Bob sends a message $M \in E({}_p)$:

1. Bob generates a random ephemeral key k.
2. Bob computes $C_1 = kP \in E({}_p)$, $C_2 = M + kQ_A \in E({}_p)$. Bob transmits the pair of points (C_1, C_2) to Alice.

Alice decrypts the message using her private key n_A:

Elliptic Curve ElGamal

Alice generates a key:

1. Choose a large prime number p, an elliptic curve E over ${}_p$, and a point $P \in E({}_p)$ of large order.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E({}_p)$.

Bob sends a message $M \in E({}_p)$:

1. Bob generates a random ephemeral key k.
2. Bob computes $C_1 = kP \in E({}_p)$, $C_2 = M + kQ_A \in E({}_p)$. Bob transmits the pair of points (C_1, C_2) to Alice.

Alice decrypts the message using her private key n_A:

1. Alice computes $C_2 - n_A C_1 \in E({}_p)$.

Key lengths for equivalent security

Key lengths for equivalent security

Symmetric Key Size	RSA Key Size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521