

Elliptic Curve Cryptography (ECC)

- ECC makes use of the elliptic curves (not ellipses) in which the variables and coefficients are all restricted to elements of a finite field.
- Two family of elliptic curves are used in ECC:
 - ▶ prime curves defined over Z_p , that is, $GF(p)$, p being a prime.
 - ▶ binary curves constructed over $GF(2^n)$.

Elliptic curves over modulo a prime $GF(p)$

Definition

Let $p > 3$ be a prime. The elliptic curve $y^2 = x^3 + ax + b$ over Z_p is the set $E_p(a, b)$ of solutions $(x, y) \in E_p(a, b)$ to the congruence

$$y^2 = x^3 + ax + b \pmod{p},$$

where $a, b \in Z_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with a special point \mathcal{O} called the point at infinity (or zero point).

Elliptic curves over modulo a prime $GF(p)$

Properties of Elliptic Curves

- An elliptic curve $E_p(a, b)$ over Z_p (p prime, $p > 3$) will have roughly p points on it.
- More precisely, a well-known theorem due to Hasse asserts that the number of points on $E_p(a, b)$, which is denoted by $\#E$, satisfies the following inequality:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

- In addition, $E_p(a, b)$ forms an abelian or commutative group under addition modulo p operation.

References

- N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
- V. Miller. Uses of elliptic curves in cryptography. Advances in Cryptology - CRYPTO'85, Lecture Notes in Computer Science (LNCS), Springer, Vol. 218, pp. 417-426, 1986.
- Douglas R. Stinson. Cryptography: Theory and Practice, Chapman & Hall/CRC, 2nd Edition, 2005.

Elliptic curves over modulo a prime $GF(p)$

Finding an inverse

- The inverse of a point $P = (x_P, y_P) \in E_p(a, b)$ is $-P = (x_P, -y_P)$, where $-y$ is the additive inverse of y .
- For example, if $p = 13$, the inverse of $(4, 2)$ is $(4, -2) \pmod{13} = (4, 11)$.

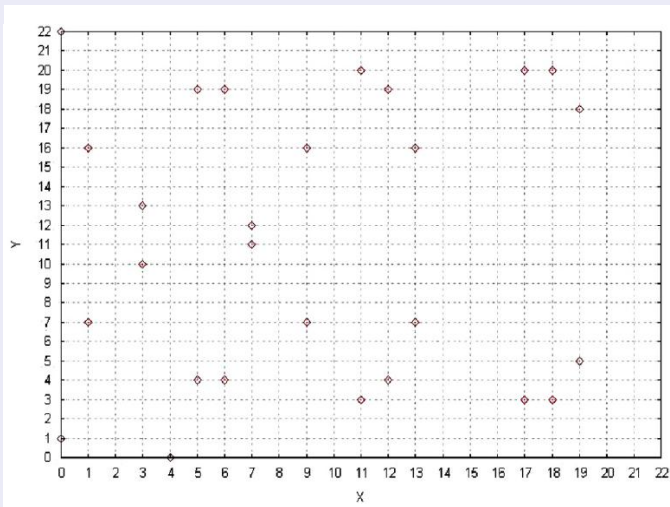
Finding all points on an elliptic curve

Algorithm: EllipticCurvePoints (p, a, b)

```
1:  $x \leftarrow 0$ 
2: while  $x < p$  do
3:    $w \leftarrow (x^3 + ax + b) \pmod{p}$ 
4:   if  $w$  is a perfect square in  $Z_p$  then
5:     Output  $(x, \sqrt{w}), (x, -\sqrt{w})$ 
6:   end if
7:    $x \leftarrow x + 1$ 
8: end while
```

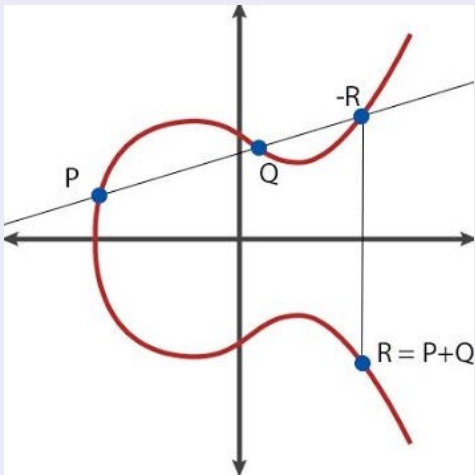
Elliptic Curve Cryptography (ECC)

Example of elliptic curve in case of $y^2 = x^3 + x + 1 \pmod{23}$.



Elliptic Curve Cryptography (ECC)

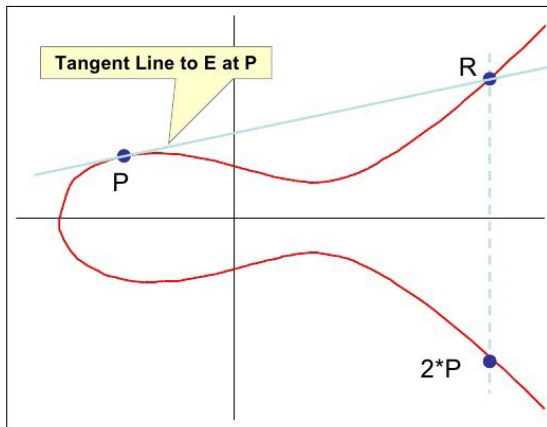
Point addition on elliptic curve over finite field $GF(p)$



Elliptic Curve Cryptography (ECC)

Doubling on elliptic curve over finite field $GF(p)$

Doubling a Point P on E



Point addition on elliptic curve over finite field $GF(p)$

Let G be the base point on $E_p(a, b)$ whose order be n , that is, $nG = G + G + \dots + G$ (n times) $= \mathcal{O}$.

If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on elliptic curve $y^2 = x^3 + ax + b \pmod{p}$, $R = (x_R, y_R) = P + Q$ is computed as follows:

$$x_R = (\lambda^2 - x_P - x_Q) \pmod{p},$$

$$y_R = (\lambda(x_P - x_R) - y_P) \pmod{p},$$

$$\text{where } \lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \pmod{p}, & \text{if } P \neq -Q \text{ [Point Addition]} \\ \frac{3x_P^2 + a}{2y_P} \pmod{p}, & \text{if } P = Q. \text{ [Point Doubling]} \end{cases}$$

Scalar multiplication on elliptic curve over finite field $GF(p)$

If $P = (x_P, y_P)$ be a point on elliptic curve $y^2 = x^3 + ax + b \pmod{p}$, then then $5P$ is computed as $5P = P + P + P + P + P$.

Think about optimization method?

Reference: N Tiwari, S Padhye. Provable Secure Multi-Proxy Signature Scheme without Bilinear Maps. International Journal of Network Security, Vol. 17, No. 1, pp. 288-293, 2015.

Elliptic Curve Cryptography (ECC)

Problem: Consider two points $P = (11, 3)$ and $Q = (9, 7)$ in the elliptic curve $E_{23}(1, 1)$. Compute $P + Q$ and $2P$.

In order to compute $R = P + Q = (x_R, y_R)$, we first compute λ as

$$\begin{aligned}\lambda &= \frac{7 - 3}{9 - 11} \pmod{23} \\ &= -2 \pmod{23} \\ &= 21.\end{aligned}\tag{1}$$

Thus, x_R and y_R are derived as

$$\begin{aligned}x_R &= (21^2 - 11 - 9) \pmod{23} = 7, \\ y_R &= (21(11 - 7) - 3) \pmod{23} = 12.\end{aligned}$$

As a result, $P + Q = (7, 12)$.

Problem: Consider two points $P = (11, 3)$ and $Q = (9, 7)$ in the elliptic curve $E_{23}(1, 1)$. Compute $P + Q$ and $2P$.

In order to compute $R = 2P = (x_R, y_R)$, we must first derive λ as follows:

$$\lambda = \frac{3(11^2) + 1}{2 \times 3} \pmod{23} = 7.$$

Hence, $R = P + P = (x_R, y_R)$ is computed as

$$\begin{aligned}x_R &= (7^2 - 11 - 11) \pmod{23} = 4, \\y_R &= (7(11 - 4) - 3) \pmod{23} = 0,\end{aligned}$$

and, thus $2P = (4, 0)$.

Elliptic Curve Computational Problems

Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Let $E_p(a, b)$ be an elliptic curve modulo a prime p .
- Given two points $P \in E_p(a, b)$ and $Q = kP \in E_p(a, b)$, for some positive integer k , where $Q = kP$ represent the point P on elliptic curve $E_p(a, b)$ be added to itself k times.
- Then the elliptic curve discrete logarithm problem (ECDLP) is to determine k given P and Q .
- It is computationally easy to calculate Q given k and P , but it is computationally infeasible to determine k given Q and P , when the prime p is large.

Elliptic Curve Discrete Logarithm Problem (ECDLP)

In other words, ECDLP can be also formally defined as follows. For any PPT algorithm, say A (in the security parameter l), $\Pr[A(P, Q) = k] < \epsilon(l)$, where $\epsilon(l)$ is a negligible function depending on l .

References:

- Vanga Odelu, **Ashok Kumar Das**, and Adrijit Goswami. “A secure effective key management scheme for dynamic access control in a large leaf class hierarchy,” in **Information Sciences (Elsevier)**, Vol. 269, No. C, pp. 270-285, 2014. (2020 SCI Impact Factor: 6.795) [This article has been downloaded or viewed 484 times since publication during the period October 2013 to September 2014]
- **Ashok Kumar Das**, Nayan Ranjan Paul, and Laxminath Tripathy. “Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem,” in **Information Sciences (Elsevier)**, Vol. 209, No. C, pp. 80 - 92, 2012. (2020 SCI Impact Factor: 6.795)

Definition (Elliptic curve computational Diffie-Hellman problem (ECCDHP))

Let $P \in E_p(a, b)$ be a point in $E_p(a, b)$. The ECCDHP states that given the points $k_1.P \in E_p(a, b)$ and $k_2.P \in E_p(a, b)$ where $k_1, k_2 \in \mathbb{Z}_p^*$, it is computationally infeasible to compute $k_1 k_2.P$, where $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$.

Definition (Elliptic curve decisional Diffie-Hellman problem (ECDDHP))

Let $P \in E_p(a, b)$ be a point in $E_p(a, b)$. The ECDDHP states that given a quadruple $(P, k_1.P, k_2.P, k_3.P)$, decide whether $k_3 = k_1 k_2$ or a uniform value, where $k_1, k_2, k_3 \in \mathbb{Z}_p^*$.

The ECDLP, ECCDHP and ECDDHP are computationally infeasible when p is large. To make ECDLP, ECCDHP and ECDDHP intractable, p should be chosen at least 160-bit prime.