Modern Complexity Theory (CS1.405)

Dr. Ashok Kumar Das

IEEE Senior Member
Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022, 2023
Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashok-kumar-das`
`https://sites.google.com/view/iitkgpakdas/`

Elliptic Curve Cryptography (ECC)

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 Curve Cryptography (ECC)

Elliptic curves over the reals

Definition

Let $a, b \in R$ be constants such that $4a^3 + 27b^2 \neq 0$. A non-singular elliptic curve is the set E of solutions $(x, y) \in R \times R$ to the equation

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

together with a special point $\mathcal{O}$ called the point at infinity (or zero point).

Elliptic Curve Cryptography (ECC)

Elliptic curves over the reals

- It can shown that the condition $4a^3 + 27b^2 \neq 0$ is the necessary and sufficient to ensure that the equation $x^3 + ax + b = 0$ has three distinct roots (may be real or complex numbers) (by Carden Method).
- If $4a^3 + 27b^2 = 0$, the corresponding elliptic curve is called singular.
- If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, then $P + Q = \mathcal{O}$ implies that $x_Q = x_P$ and $y_Q = -y_P$.
- Also, $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E$.

Elliptic Curve Cryptography (ECC)

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

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 $4a^3 + 27b^2 \neq 0 \pmod{p}$, 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.

Elliptic Curve Cryptography (ECC)

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, 2^{nd} Edition, 2005.

Elliptic Curve Cryptography (ECC)

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 $(4, -2) \pmod{13}$ $= (4, 11)$.

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

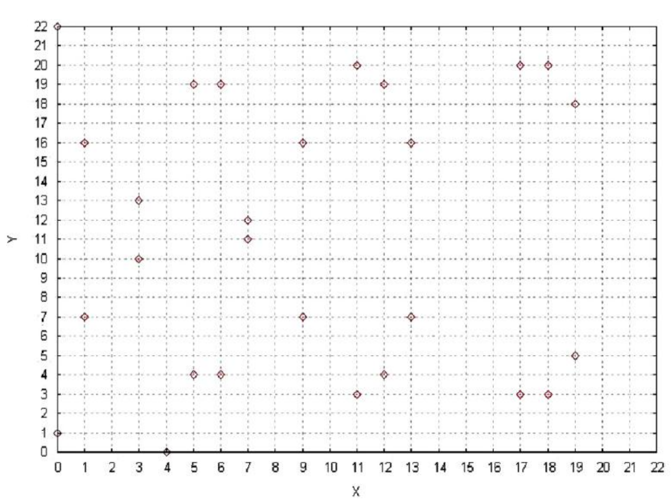
Finding all points on an elliptic curve

Algorithm: EllipticCurvePoints (p, a, b)

$x \leftarrow 0$
while $x < p$ **do**
    $w \leftarrow (x^3 + ax + b) \pmod{p}$
    if w is a perfect square in Z_p) **then**
        Output $(x, \sqrt{w}), (x, -\sqrt{w})$
    end if
    $x \leftarrow x + 1$
end while

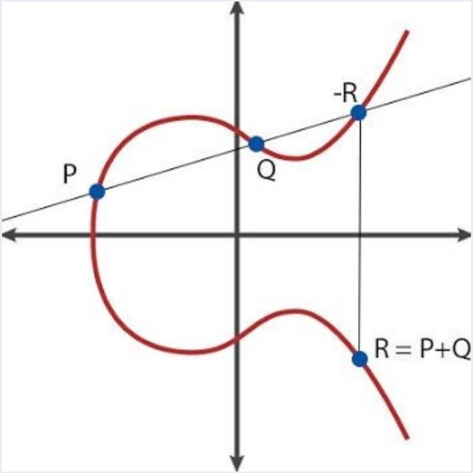
Elliptic Curve Cryptography (ECC)

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



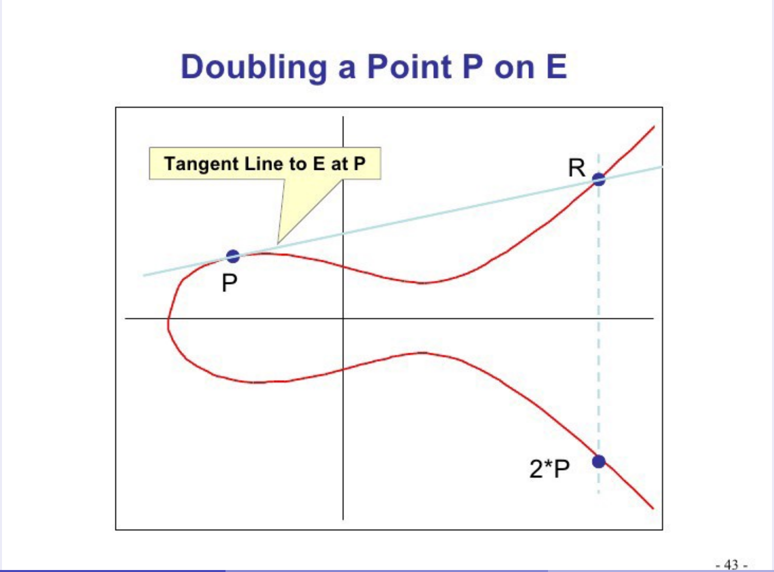
Elliptic Curve Cryptography (ECC)

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



Elliptic Curve Cryptography (ECC)

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



Elliptic Curve Cryptography (ECC)

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

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

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:

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

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

Elliptic Curve Cryptography (ECC)

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 $5P$ 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

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

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

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 $R = 2P = (x_R, y_R)$, 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

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

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

Elliptic Curve Cryptography (ECC)

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 Cryptography (ECC)

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Definition

Let $E_p(a, b)$ be an elliptic curve modulo a prime p, and $P \in E_p(a, b)$ and $Q = kP \in E_p(a, b)$ be two points, where $k \in_R Z_p^* = \{1, 2, \cdots, p-1\}$ (We use the notation $a \in_R B$ to denote that a is randomly chosen from the set B).

Instance: (P, Q, m) for some $k, m \in_R Z_p^*$.

Output: **Yes**, if $Q = mP$, i.e., $k = m$, and **No**, otherwise.

Consider the following two probability distributions:

$$\begin{aligned} D_{real} &= \{k \in_R Z_p, U = P, V = Q(= kP), W = k : (U, V, W)\}, \text{ and} \\ D_{rand} &= \{k, m \in_R Z_p, U = P, V = Q(= kP), W = m : (U, V, W)\}. \end{aligned}$$

Elliptic Curve Cryptography (ECC)

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Definition

The advantage of any probabilistic polynomial-time (PPT), 0/1-valued distinguisher $\mathcal{D}$ in solving *ECDLP* on $E_p(a, b)$ is defined as

$$
\begin{aligned}
Adv^{ECDLP}_{\mathcal{D},E_p(a,b)} \quad = \quad & |Pr[(U, V, W) \leftarrow D_{real} : \mathcal{D}(U, V, W) = 1] \\
& -Pr[(U, V, W) \leftarrow D_{rand} : \mathcal{D}(U, V, W) = 1]|,
\end{aligned}
$$

where the probability $Pr[\cdot]$ is taken over the random choices of k and m. $\mathcal{D}$ is called an (t, ϵ)-ECDLP distinguisher for $E_p(a, b)$ if $\mathcal{D}$ runs at most in time t with $Adv^{ECDLP}_{\mathcal{D},E_p(a,b)}(t) \geq \epsilon$.

ECDLP assumption: There exists no (t, ϵ)-ECDLP distinguisher for $E_p(a, b)$. Thus, for every $\mathcal{D}$, $Adv^{ECDLP}_{\mathcal{D},E_p(a,b)}(t) \leq \epsilon$, with atmost time t.

Elliptic Curve Cryptography (ECC)

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. (2019 SCI Impact Factor: 5.910) [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. (2019 SCI Impact Factor: 5.910)

Elliptic Curve Cryptography (ECC)

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 $k_1, k_2 \in Z_p^*$, it is computationally infeasible to compute $k_1 k_2.P$, where $Z_p^* = \{1, 2, \cdots, p-1\}$.

Elliptic Curve Cryptography (ECC)

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 $k_1, k_2, k_3 \in Z_p^*$.

Elliptic curve-based computationally hard problems

It is known that ECDLP, ECCDHP and ECDDHP are computationally intractable when q is large. More precisely, the value of q should be selected at least 160-bit prime to ensure that ECDLP, ECCDHP and ECDDHP are computationally infeasible.

Lemma

$ECDLP \leq_p ECCDHP \leq_p ECDDHP$.

Proof.

* Let R be a point in $E_p(a, b)$ and given two points $i \cdot R \in E_p(a, b)$ and $j \cdot R \in E_p(a, b)$. Given $i \cdot R$ and $j \cdot R$, using the ECDLP, one can determine $i, j \in Z_q^*$, if ECDLP can be solved in polynomial time. Hence, we can compute $(i * j) \cdot R$. Thus, ECDLP $\leq_p$ ECCDHP.
* Let R be a point in $E_p(a, b)$ and given a quadruple (R, $i \cdot R$, $j \cdot R$, $k \cdot R$). If the ECCDHP can be solved in polynomial-time, we can determine $(i * j) \cdot R$ from $i \cdot R$ and $j \cdot R$. Then, we can check if $(i * j) \cdot R$ $= k \cdot R$. If it is so, $k = i * j$. Thus, ECCDHP $\leq_p$ ECDDHP. $\square$