Cryptography
ECE5632 - Spring 2025

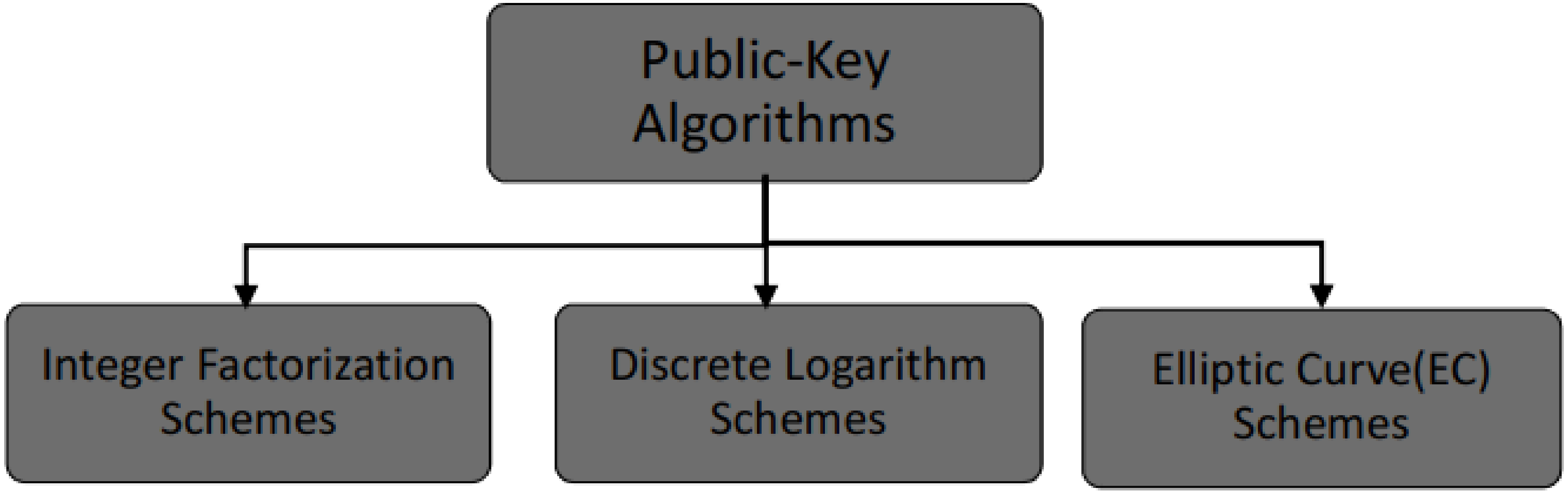
Lecture 9A

Dr. Farah Raad

Lecture Topic

Elliptic Curve Cryptography

PKC Algorithms: Three Families



e.g.
- RSA algorithm.

e.g.:
- Diffie–Hellman key exchange.
- ElGamal encryption.
- Digital Signature Algorithm (DSA).

e.g.:
- EC Diffie–Hellman key exchange (ECDH).
- EC Digital Signature Algorithm (ECDSA).

Elliptic Curve Cryptography

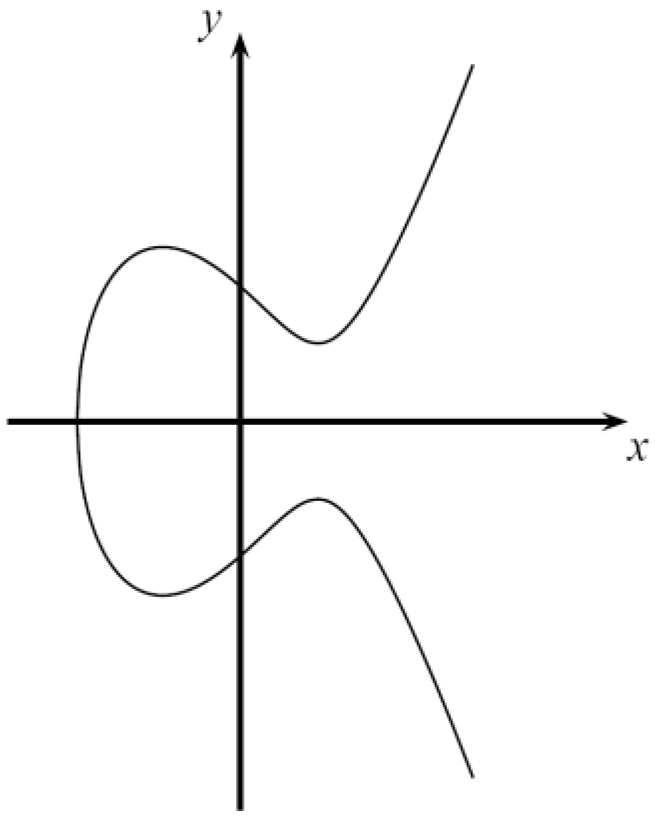
Problem:
Asymmetric schemes like RSA and Elgamal require exponentiations in integer rings and fields with parameters of more than 1000 bits.

- High computational effort on CPUs with 32-bit or 64-bit arithmetic
- Large parameter sizes critical for storage on small and embedded

Motivation:
Smaller field sizes providing equivalent security are desirable

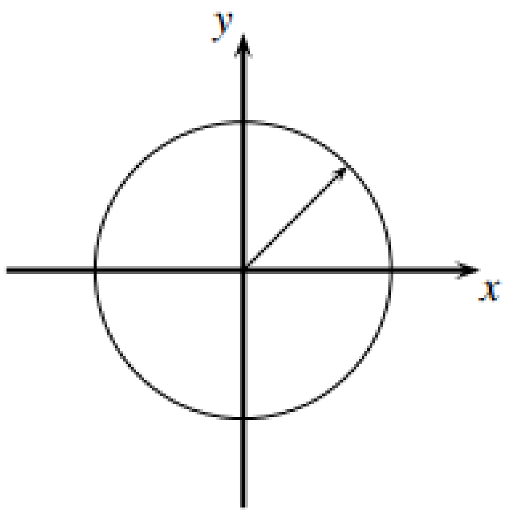
Solution:
Elliptic Curve Cryptography uses a group of points (instead of integers) for cryptographic schemes with coefficient sizes of 160-256 bits, reducing significantly the computational effort.

ECC is based on the generalized discrete logarithm problem.

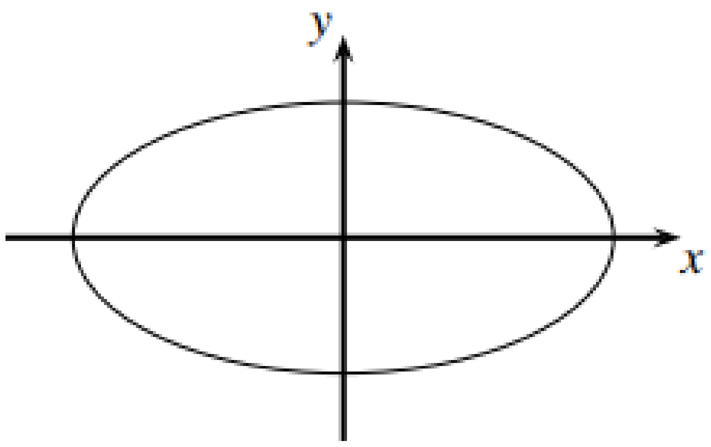


Elliptic Curve Cryptography

polynomial equations over the real numbers.



Plot of all points (x, y) which fulfill the equation $x^2 + y^2 = r^2$ over $\mathbb{R}$



Plot of all points (x, y) which fulfill the equation $a \cdot x^2 + b \cdot y^2 = c$ over $\mathbb{R}$

Elliptic Curve Cryptography

- From the two examples above, we conclude that we can form certain types of curves from polynomial equations.
- An *elliptic curve* is a special type of polynomial equation.
- In cryptography, we are interested in elliptic curves module a prime *p*:

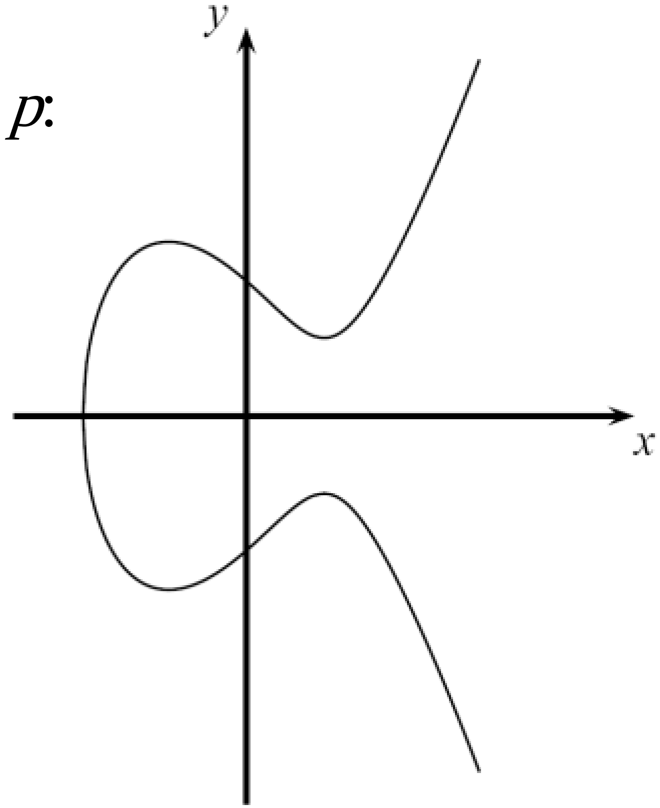
Definition 9.1.1 Elliptic Curve
The elliptic curve *over* $\mathbb{Z}_p$, $p > 3$, *is the set of all pairs* $(x, y) \in \mathbb{Z}_p$ *which fulfill*

$$y^2 \equiv x^3 + a \cdot x + b \bmod p$$

together with an imaginary point of infinity $\mathcal{O}$, *where*

$$a, b \in \mathbb{Z}_p$$

and the condition $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \bmod p$.



- Note that $Z_p = \{0, 1, \ldots, p-1\}$ is a set of integers with modulo p arithmetic

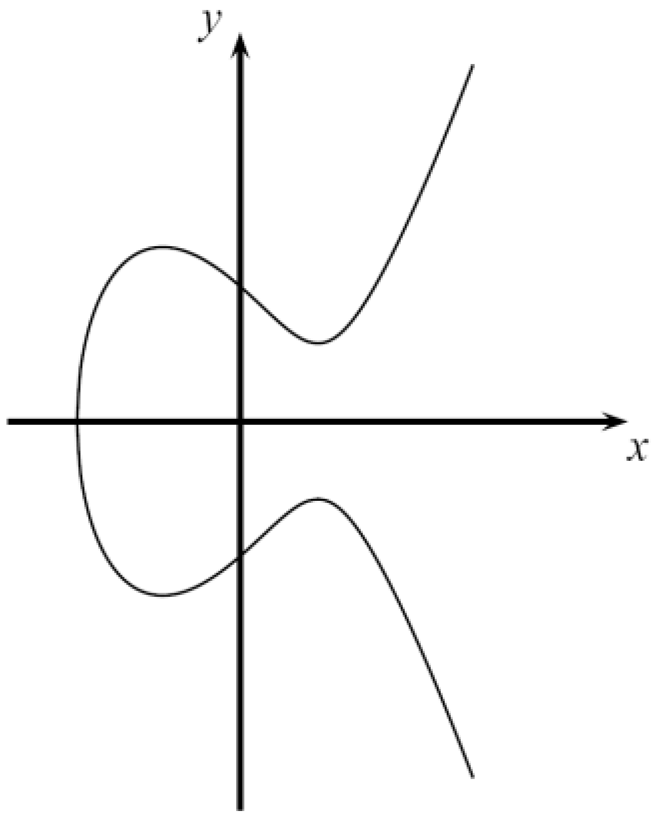
Elliptic Curve Cryptography

- Elliptic curves are polynomials that define points based on the (simplified) Weierstrass equation:

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

for parameters a,b that specify the exact shape of the curve

- On the real numbers and with parameters a, b R, an elliptic curve looks like this à



- Elliptic curves can not just be defined over the real numbers *R* but over many other types of finite fields.

Elliptic Curve Cryptography

$$P = (x_1, y_1) \text{ and } Q = (x_2, y_2)$$

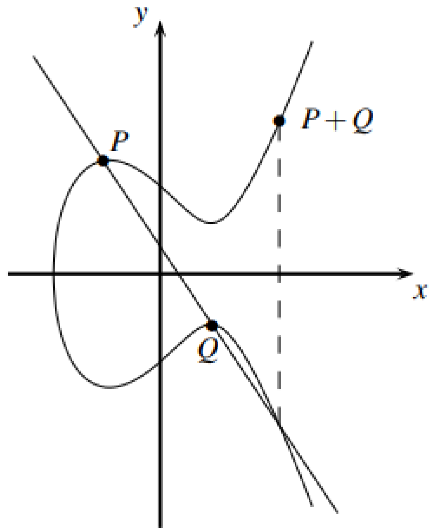
$$P + Q = R$$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

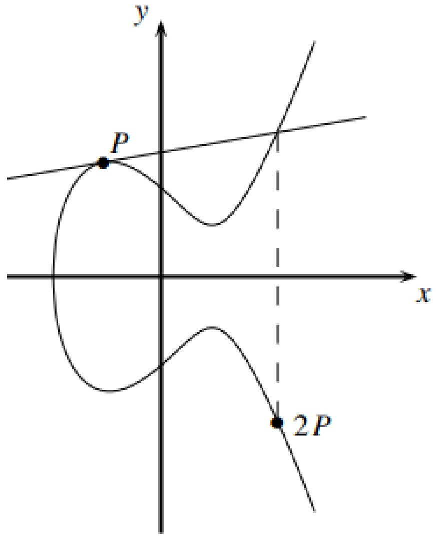
Point Addition P+Q This is the case where we compute $R = P + Q$ and $P \neq Q$.

The construction works as follows: Draw a line through P and Q and obtain a third point of intersection between the elliptic curve and the line.

Point Doubling P+P This is the case where we compute $P+Q$ but $P = Q$. Hence, we can write $R = P+P = 2P$.



Point addition on an elliptic curve over the real numbers



Point doubling on an elliptic curve over the real numbers

Elliptic Curve Cryptography

Elliptic Curve Point Addition and Point Doubling

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

Elliptic Curve Cryptography

Example :

Consider the Elliptic curves Weierstrass equation is : $y^2 = x^3 + 3x + 10\ (mod 29)$

let P=(5,11) , Q=(10, 24),

1. Add the points P, Q.
2. Double the point P.

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

Answer:

From Elliptic equation, we have a= 3 , b=10 , *P*=29

1. For Adding points P, Q , we should calculate S to be able calculate R

$$P + Q = R$$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$S = \frac{y_2 - y_1}{x_2 - x_1}\ mod\ p$$

$$S = \frac{24 - 11}{10 - 5}\ mod\ 29 = 13\ * (5)^{-1}\ mod\ 29 = 13 * 6\ mod 29 = 20$$

$$x_3 = s^2 - x_1 - x_2 \bmod\ p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod\ p$$

$x_3 = 8\ \ , y_3 = 16$

R=(8,16)

Elliptic Curve Cryptography

Example :

Consider the Elliptic curves Weierstrass equation is : $y^2 = x^3 + 3x + 10\ (mod29)$

let P=(5,11) , Q=(10, 24),

1. Add the points P, Q.
2. Double the point P.

Answer:

2. For Doubling point P, we should calculate S to be able calculate R $R = P + P = 2P$.

$$S = \frac{3x_1^2 + a}{2y_1}\ mod\ p$$

$$S = \frac{3(5)^2+3}{2 * 11}\ mod\ 29 = \frac{78}{22}\ mod29 = \frac{78mod29}{22mod29} mod29 = 20 \ * 22^{-1} mod29 = 20 * 4mod29$$
$$= 80\ mod29 = 22$$

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

$$x_3 = 10 \quad , y_3 = 24$$

R=(10, 24)

Elliptic Curves Diffie–Hellman Key Exchange

ECDH Domain Parameters

1. Choose a prime p and the elliptic curve

$$E : y^2 \equiv x^3 + a \cdot x + b \bmod p$$

2. Choose a primitive element $P = (x_P, y_P)$

The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters.

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		**Bob**
choose $k_{prA} = a \in \{2, 3, \ldots, \#E - 1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E - 1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

Elliptic Curves Diffie–Hellman Key Exchange

The correctness of the protocol is easy to prove.

Proof. Alice computes

$$aB = a(bP)$$

while Bob computes

$$bA = b(aP).$$

Elliptic Curve Digital Signature Algorithm (ECDSA)

Key Generation for ECDSA

1. Use an elliptic curve E with
   - modulus p
   - coefficients a and b
   - a point A which generates a cyclic group of prime order q
2. Choose a random integer d with $0 < d < q$.
3. Compute $B = d\,A$.

The keys are now:

$k_{pub} = (p, a, b, q, A, B)$

$k_{pr} = (d)$

Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA Signature Generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $R = k_E A$.
3. Let $r = x_R$.
4. Compute $s \equiv (h(x) + d \cdot r) k_E^{-1} \bmod q$.

ECDSA Signature Verification

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot h(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $P = u_1 A + u_2 B$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$x_P \begin{cases} \equiv r \bmod q \Longrightarrow \text{valid signature} \\ \not\equiv r \bmod q \Longrightarrow \text{invalid signature} \end{cases}$$

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!

Any Question?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt

Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451

Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg