A Relation between Group Order of Elliptic Curve and Extension Degree of Definition Field

Taichi Sumo, Yuki Mori (Okayama University)

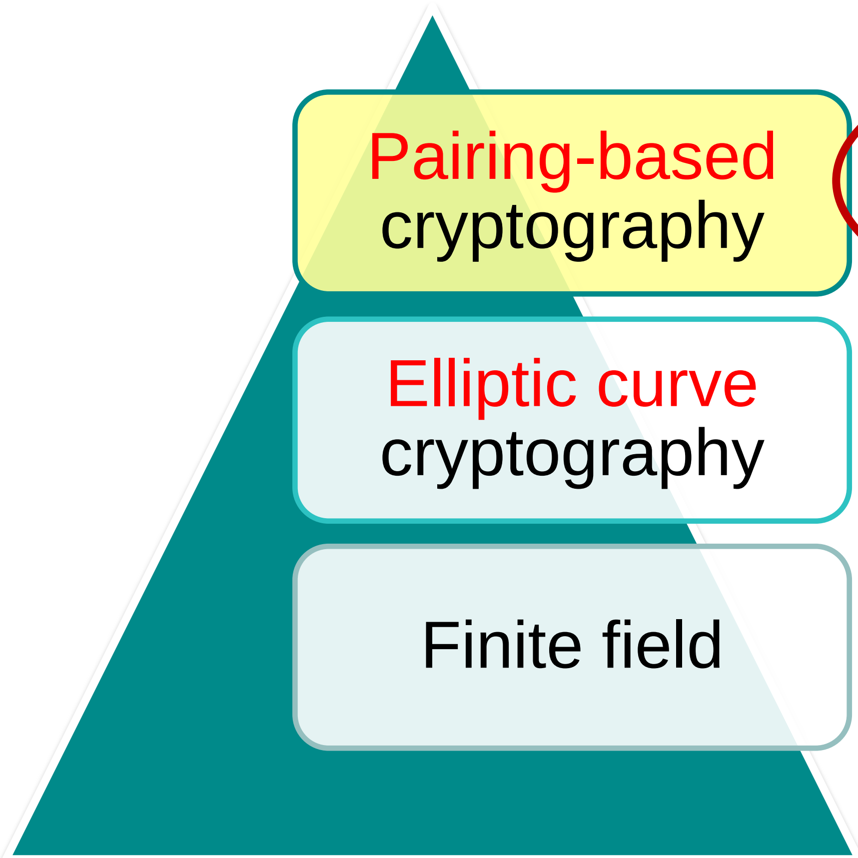
Yasuyuki Nogami (Graduate School of Okayama University)

Tomoko Matsushima (Polytechnic University)

Satoshi Uehara (University of Kitakyushu)

Research Background

Recent innovative cryptographic applications are based on …



- **ID-based cryptography**
- **Group signature authentication**
- **Time release cryptography**

- **EC discrete logarithm problem**
  - **Elliptic curve addition**

- **Prime field and Extension field**
- **Arithmetic operations**
  - **Addition/Subtraction**
  - **Multiplication/Division**

Research Background

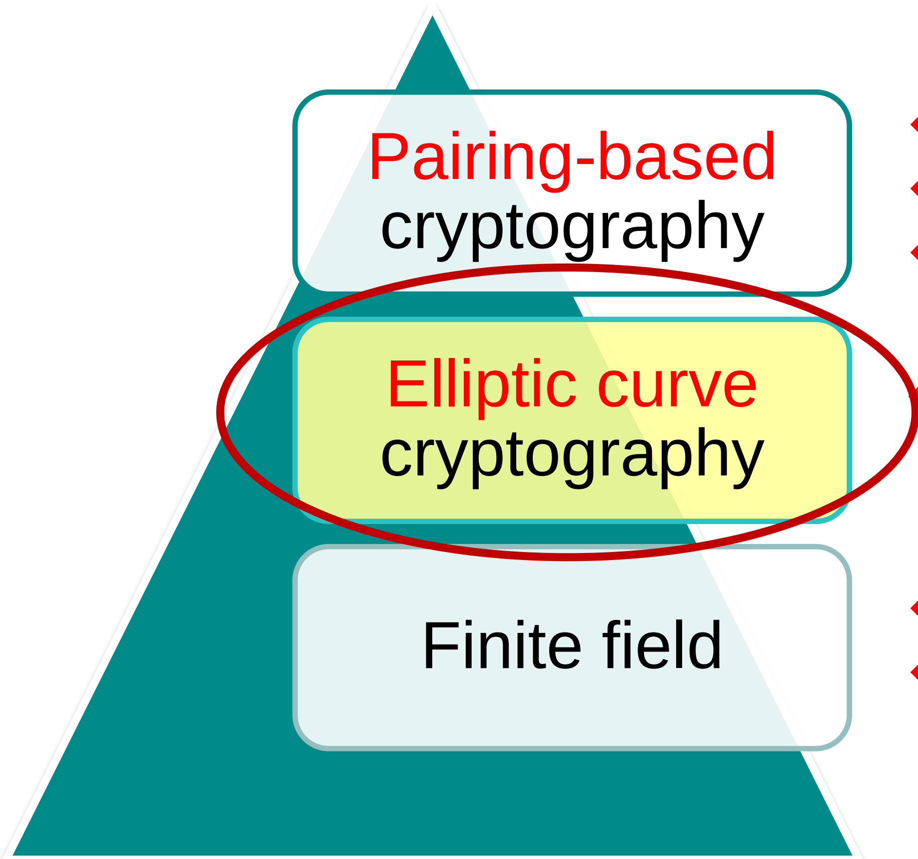
- ID-based cryptography
  - We can use ID-based information as public key.
    - User name
    - E-main address
    - Phone number etc.

- Group signature authentication
  - Anonymous authentication
  - Attribute-based authentication

- Time release cryptography
  - It keeps the data encrypted until the day for release comes.

Research Background

Pairing-based cryptography is based on elliptic curve cryptography.



- **ID-based cryptography**
- **Group signature authentication**
- **Time release cryptography**

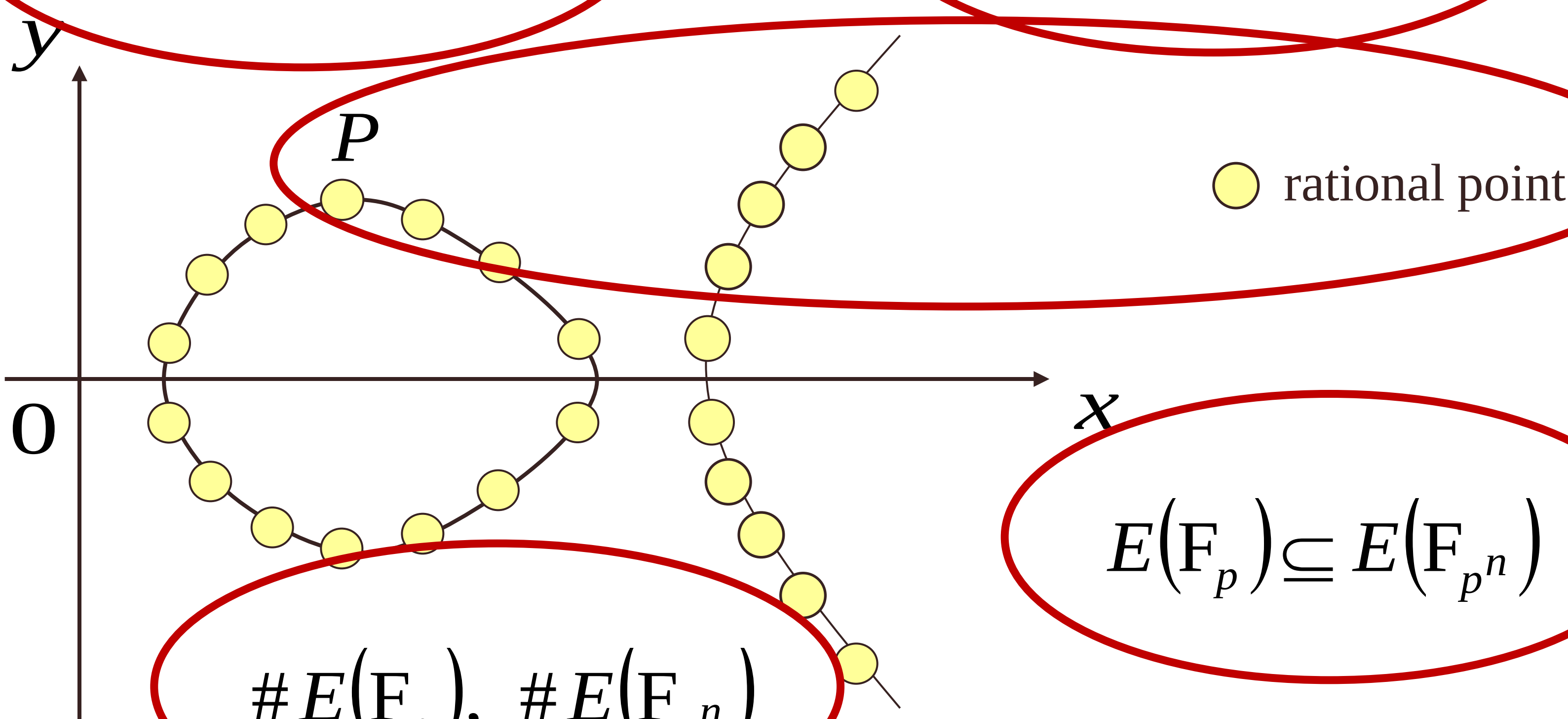
- **EC discrete logarithm problem**
  - **Elliptic curve addition**

- **Extension field**
- **Arithmetic operations**
  - **Addition**
  - **Multiplication**

*Finite and discrete mathematics

Mathematical notations

$$E : y^2 = x^3 + ax + b, \quad a, b, x, y \in \mathrm{F}_{p^n} \qquad \mathrm{F}_p \subseteq \mathrm{F}_{p^n}$$



$$E(\mathrm{F}_p) \subseteq E(\mathrm{F}_{p^n})$$

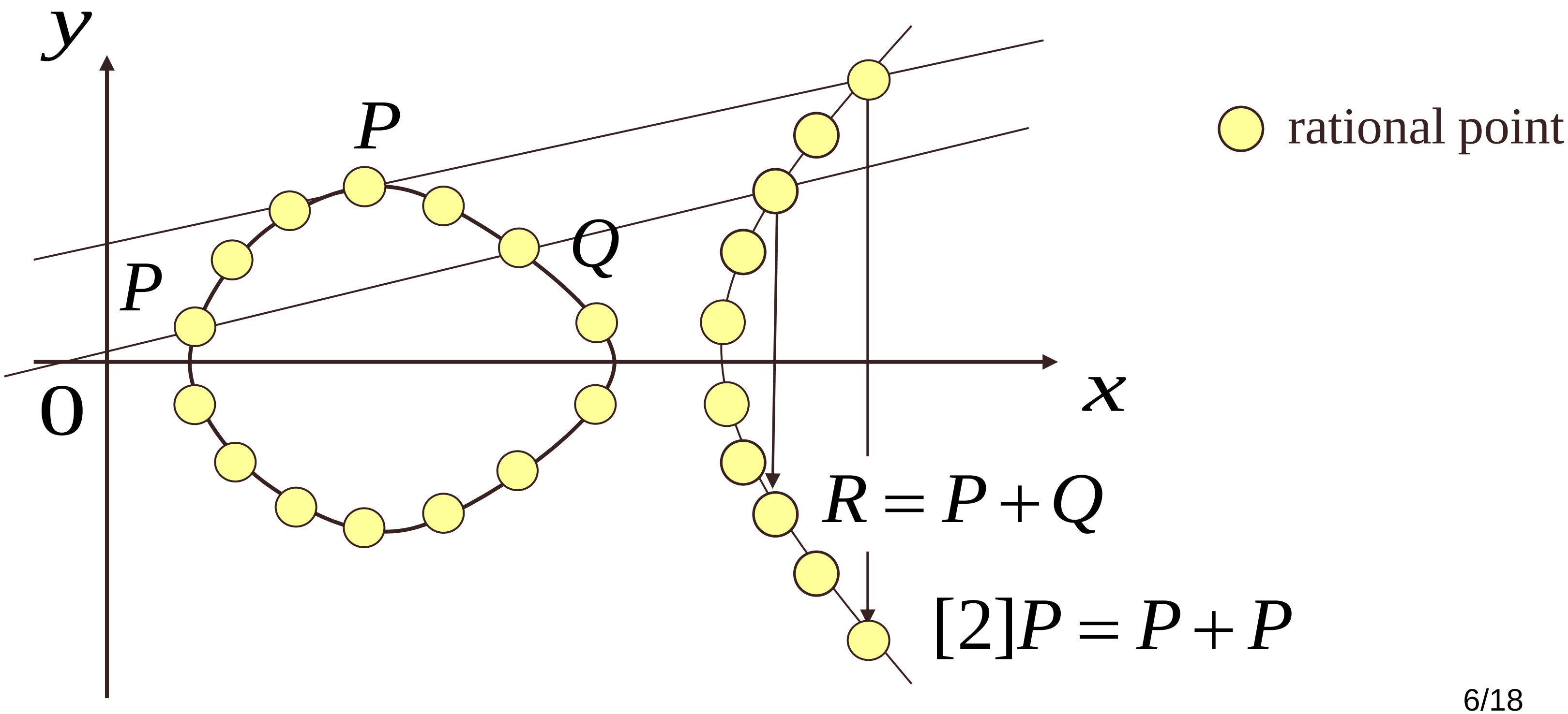
$$\# E(\mathrm{F}_p), \ \# E(\mathrm{F}_{p^n})$$

Elliptic curve cryptography (1/2)

Elliptic curve cryptography

Arithmetic operations

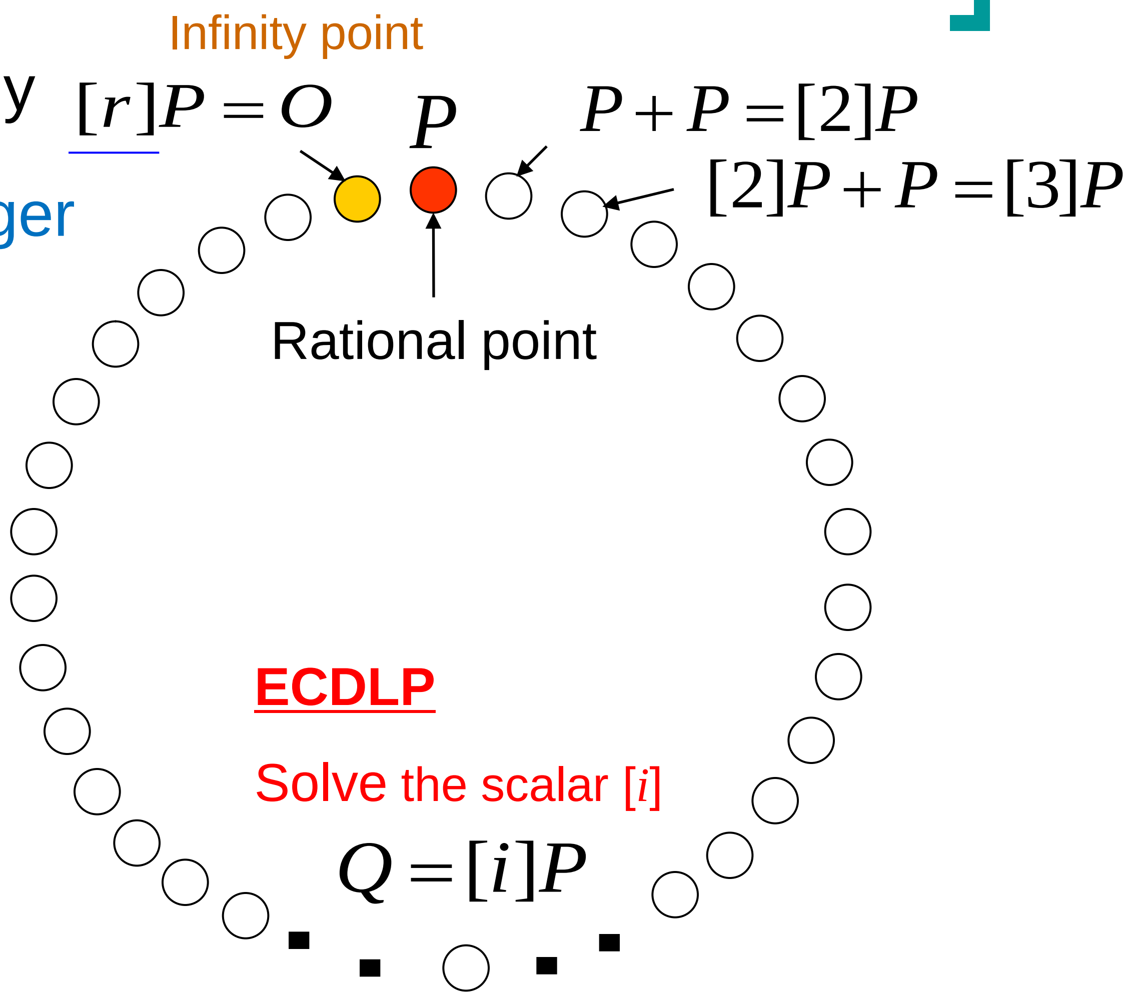
$$E: y^2 = x^3 + ax + b, \quad a, b, x, y \in \mathrm{F}_{p^n}$$



Elliptic curve cryptography (2/2)

Elliptic curve cryptography

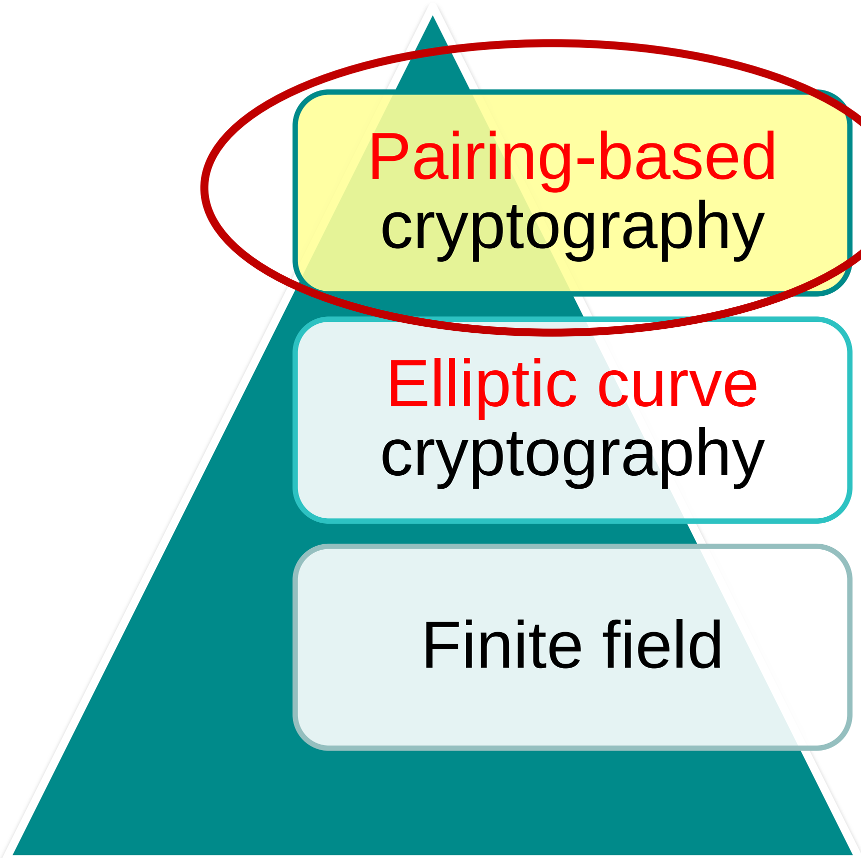
the order r is larger than 160 bits



Cyclic group

Research Background

Pairing-based cryptography uses a special class of elliptic curve.



- **ID-based cryptography**
- **Group signature authentication**
- **Time release cryptography**

- **EC discrete logarithm problem**
  - **Elliptic curve addition**

- **Extension field**
- **Arithmetic operations**
  - **Addition**
  - **Multiplication**

Pairing-based cryptography (1/3)

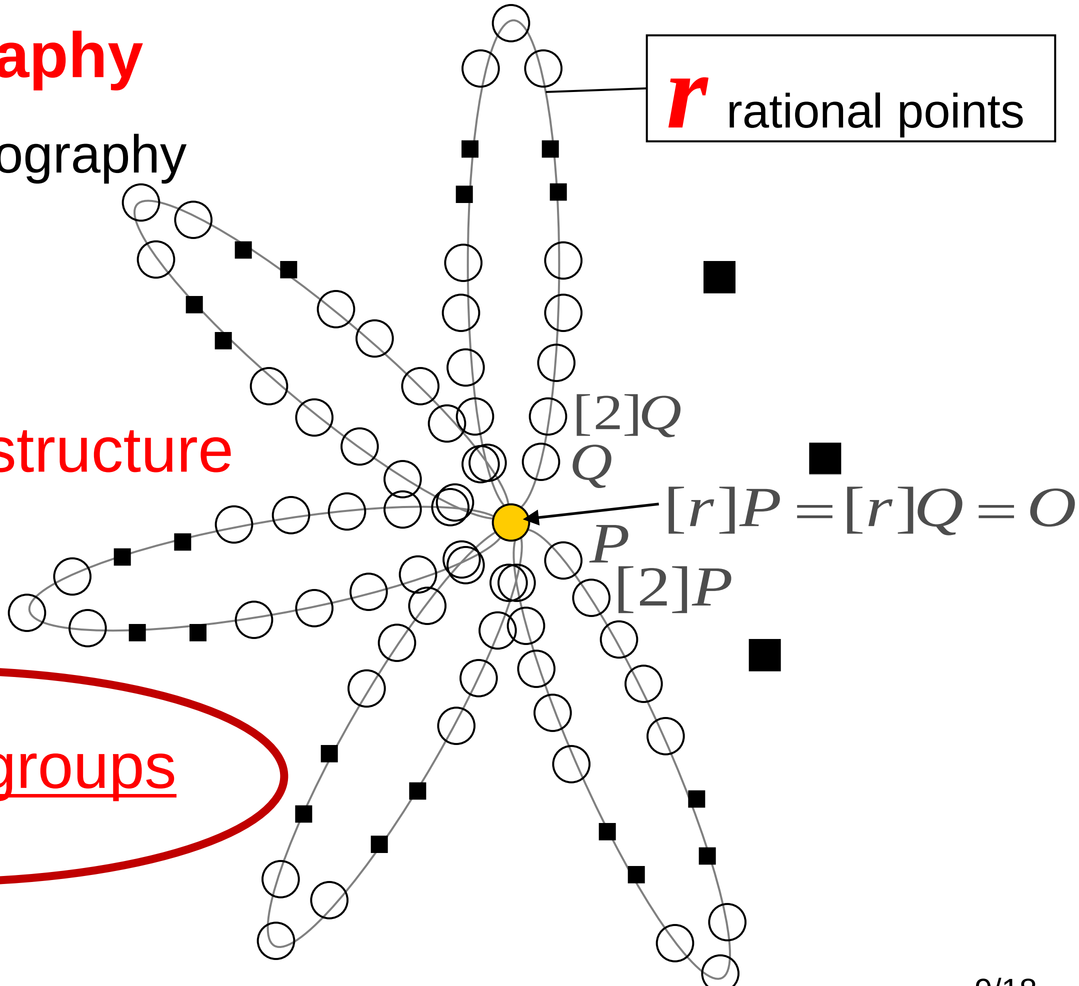
Pairing-based cryptography

over elliptic curve cryptography

Requirement:
torsion group structure

Pairing uses two cyclic groups

among $r+1$



Pairing-based cryptography (2/3)

- Pairing-friendly curves
  - It is defined over extension field F_{p^n} ***n*-th vector space**
  - The defining equation is

$$E: y^2 = x^3 + ax + b, \quad a, b, x, y \in F_{p^n}$$

- Some conditions should be satisfied
  - Torsion group structure
  - The number of rational points $\#E(F_{p^n})$

needs to be divisible by r^2.

Pairing-based cryptography (3/3)

- How to prepare pairing-friendly curves
  - It is difficult except for some special curves
    - Barreto-Naehrig (BN) curve : $n = 12$
    - Brezing-Weng (BW) curve : $n = 8$

- Setting parameters :
  - ***p, a, b***
  - #rational points ***r***
  - dimension ***n***

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

$$a, b, x, y \in \mathrm{F}_{p^n}$$

$$\#E\left(\mathrm{F}_{p^n}\right) \quad r$$

Target of this research

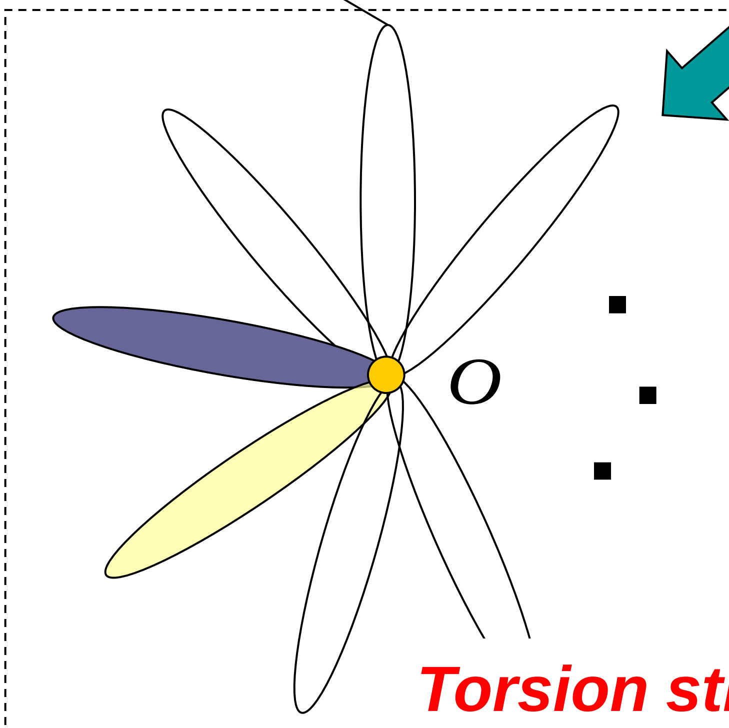
There are r points in each cyclic group

n : the extension degree (dimension)

$$n \mid (r-1)$$

There are some previous works.

BN and BW curves



Torsion structure

$$n \nmid (r-1)$$

There are few reports

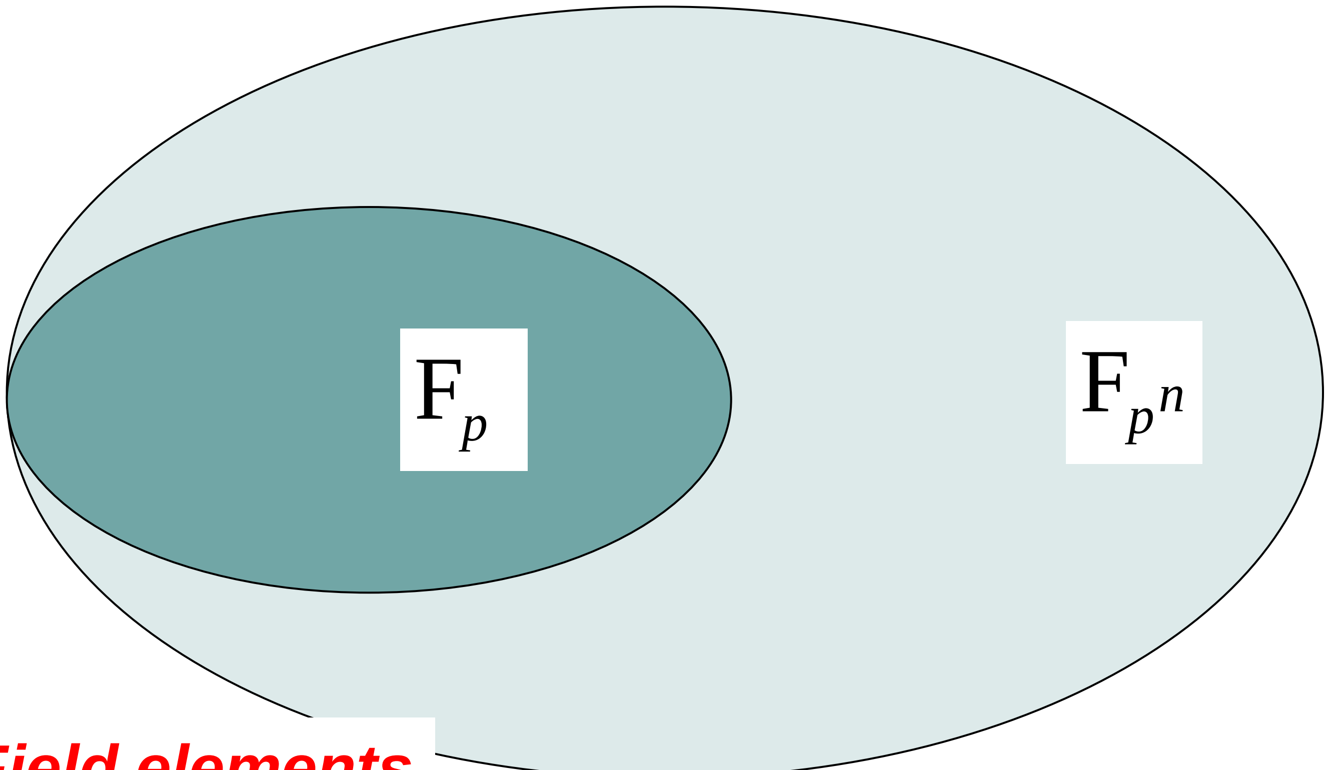
$$n \mid (r+1)$$

$$n = r$$

The target of this work

Algebraic closure

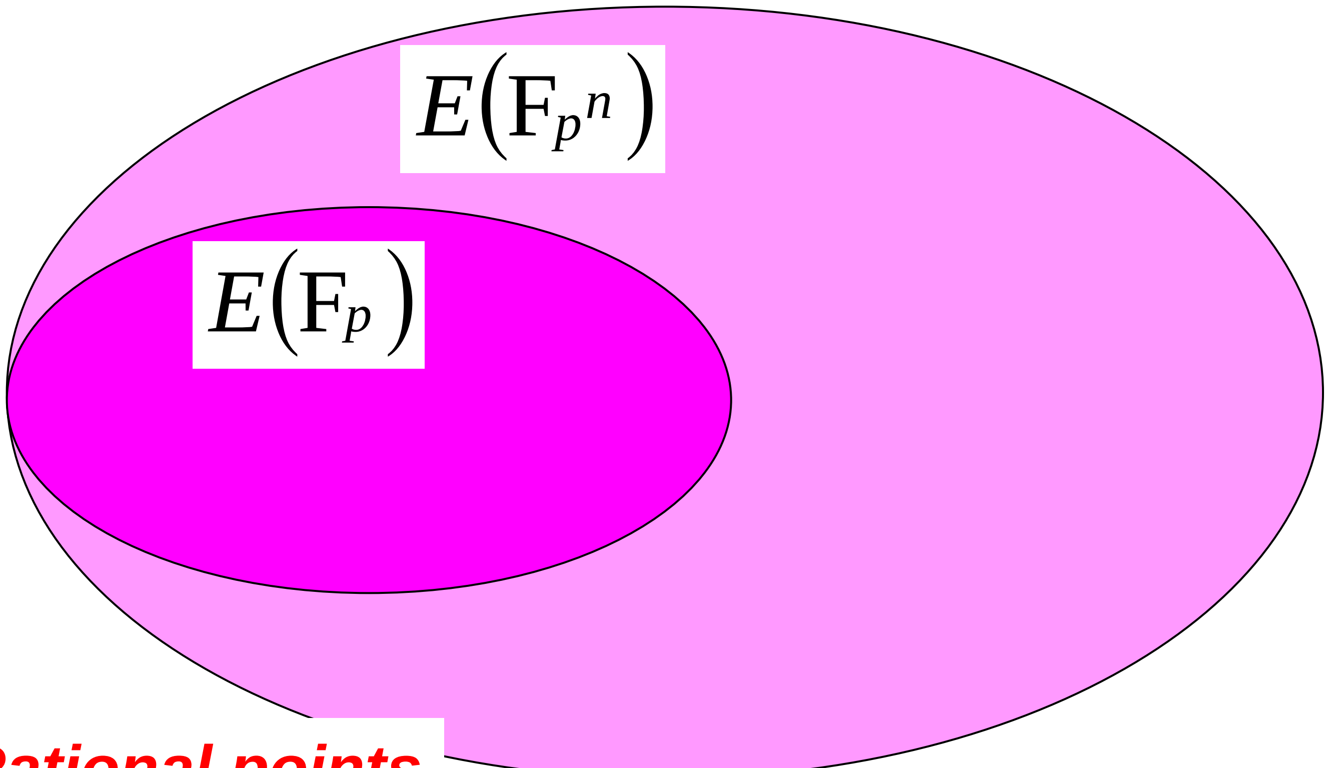
- Prime field F_p and n-th Extension field F_{p^n}



: Field elements

In the same Elliptic curve closure

- Over Prime field $E(\mathrm{F}_p)$ and ex. field $E(\mathrm{F}_{p^n})$

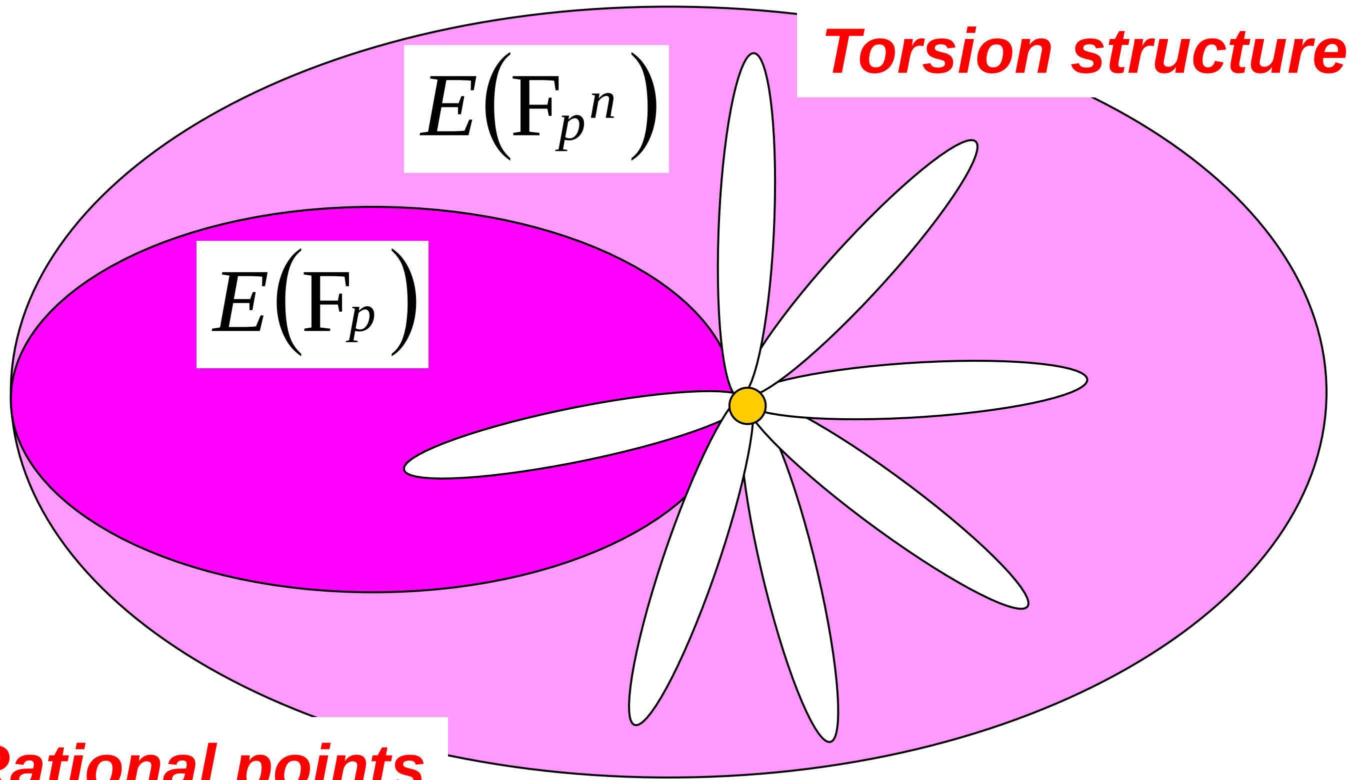


: Rational points

Our contribution (theoretic proof was given)

- <u>If</u> $r \mid \# E(\mathrm{F}_p)$ <u>and</u> $n = r$

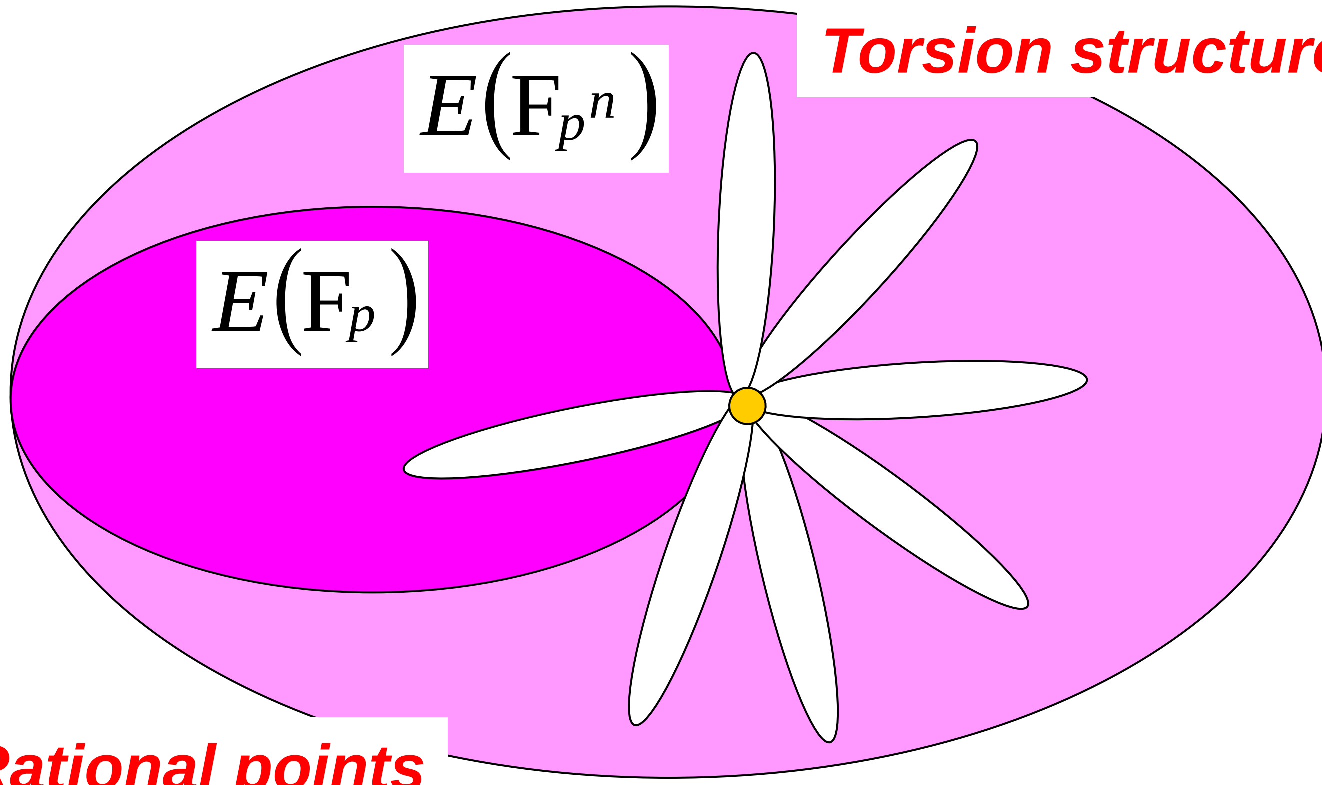
Torsion structure appears



: Rational points

Our contribution (theoretic proof was given)

- <u>If</u> $r \mid \#E(\mathbb{F}_p)$ <u>and</u> $n = r$



Example

Example 1:

$$p = 11, \quad r = 5,$$
$$E : \; y^2 = x^3 + 6x + 3,$$
$$\#E(\mathbb{F}_p) = 15, \quad \#E(\mathbb{F}_{p^5}) = 161625.$$

Conclusion

- This work has focused on $n = r$
  - Torsion structure appears

- Further consideration
  - Consider pairing-based cryptographic applications.

Thank you for your attentions.