§ Cryptographic Hashing Functions

① MiMC5 Sponge (H_2)

Description: MiMC5 operating in Feistel mode with sponge construction.

Behavior: $(\mathbb{Z}_p, \mathbb{Z}_p) \rightarrow \mathbb{Z}_p$

Implementation: Circom, Solidity (in the form of a Hasher contract)

② Pedersen (H_1)

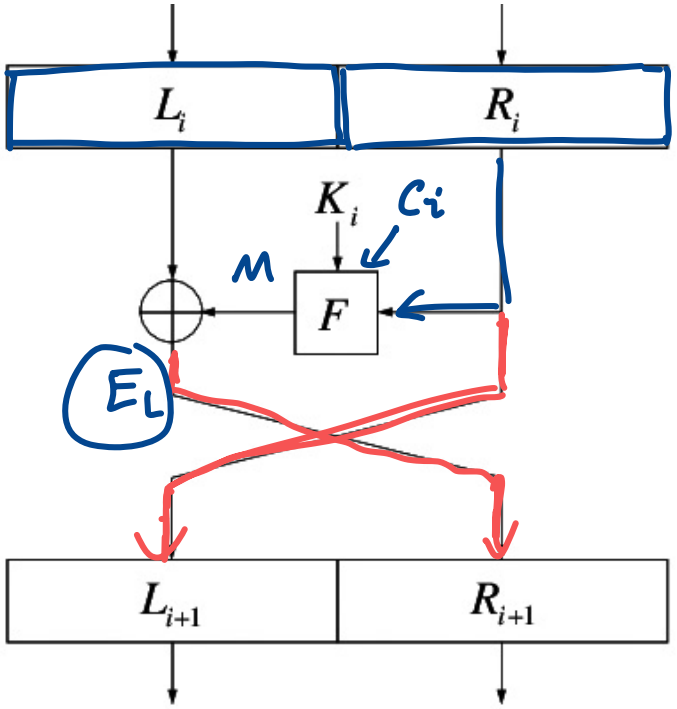
Description: Bit-wise hashing function (4-bit window)

Behavior: $\mathbb{B}^* \rightarrow \mathbb{Z}_p$ (x-coordinate of a point on an elliptic curve)

Implementation: Circom.

§ Feistel Construction

- 2 inputs → 2 outputs



① R_i, K_i, C_i → F → M

Mask for encryption

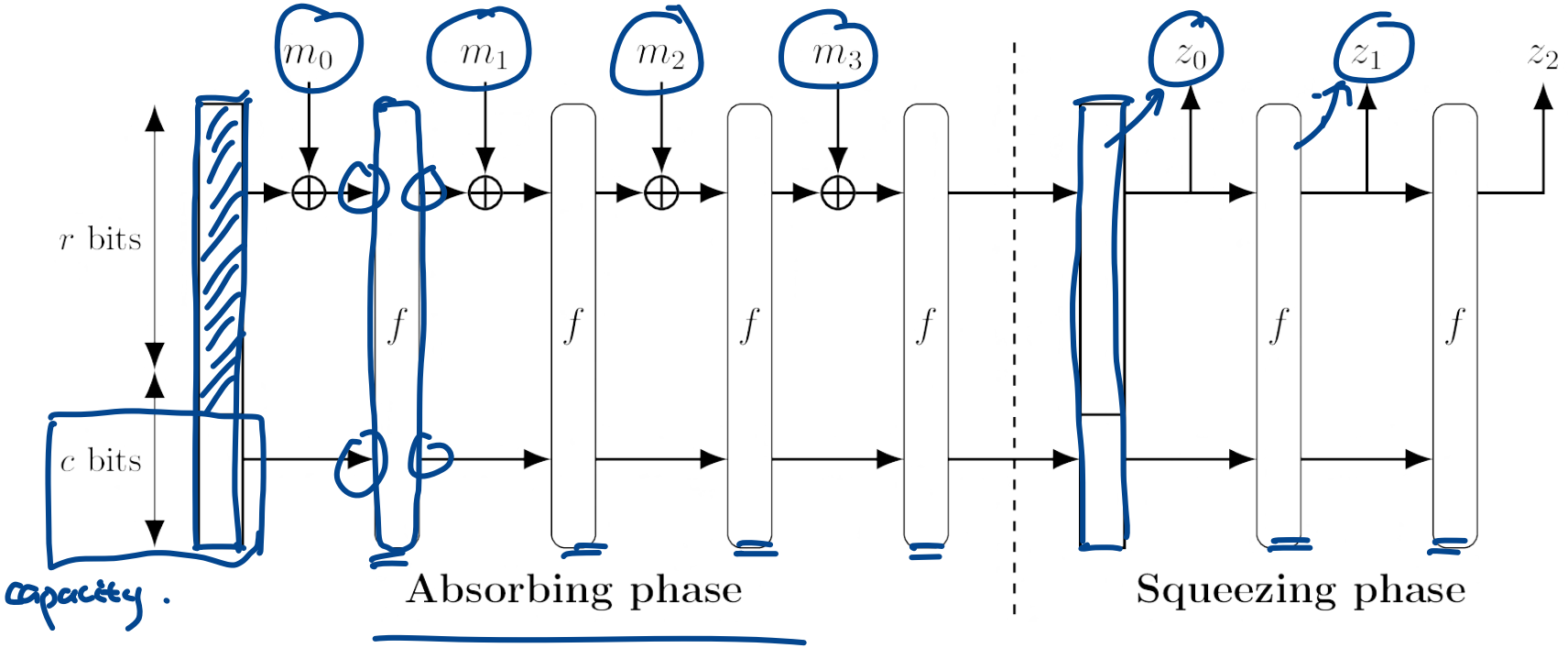
② M, L_i → ⊕ → E_L

③ Exchange place

F is MiMC5,

$M = (R_i + K_i + C_i)^5$

§ Sponge



capacity.

- f is an encryption routine
- the state of encryption is split: r bits (actively taking inputs/output)
  c bits capacity
- f: 2 inputs, 2 outputs
- MiMCSponge. f is MiMC5 Feistel

§ Elliptic Curve Cryptography

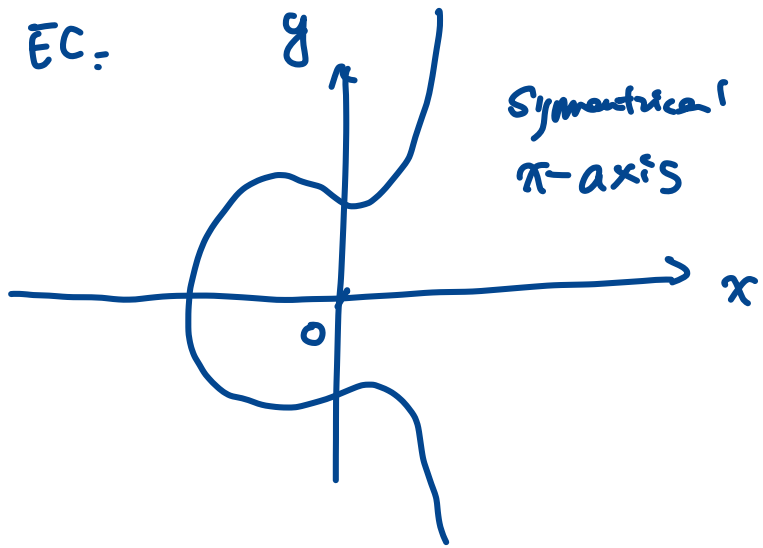
① What is a Group?

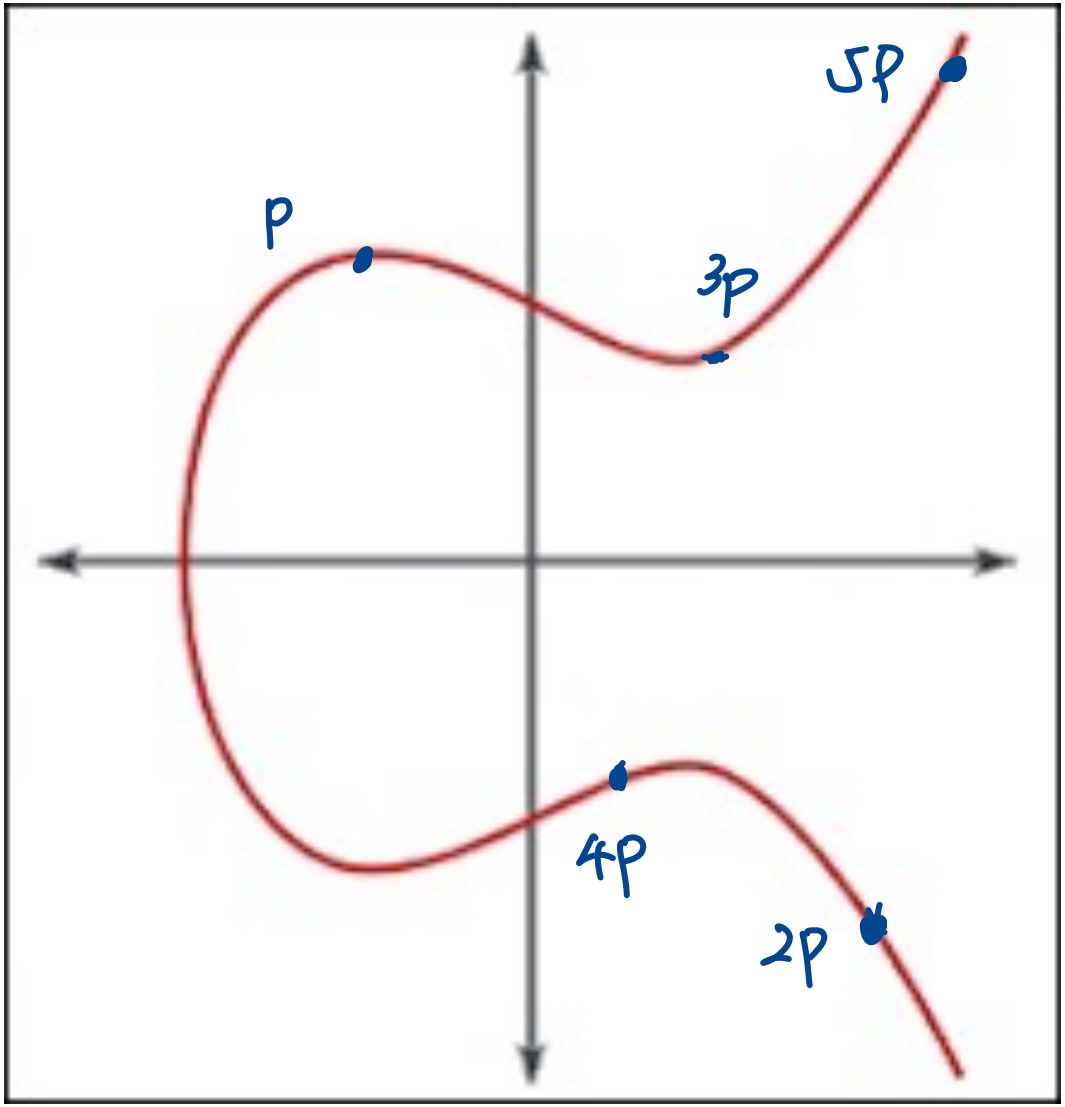
- A set of elements
- Well-defined addition

② Points on an elliptic curve with coordinates $\in \mathbb{Z}_p$

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

③ EC:





EC: $y^2 = x^3 - x + 3$