# Geometry in Cryptography

Luca Giuzzi

Summer School

Giuseppe Tallini

9 July 2004

## Cryptosystems

- $M$ set of messages
- $K$ set of keys
- $C$ set of cyphertexts
- $e : M \times K \mapsto C$ encryption
- $d : C \times K \mapsto M$ decryption

$$\forall k \in K : \exists k' \in K$$
such that
$$\forall m \in M : d(e(m, k), k') = m.$$

## Discrete Logarithm Problem

- $\mathcal{G} = \langle g \rangle$ group
- $m \in \mathcal{G}$

Determine

$\alpha \in \mathbb{N}$ such that
$m = g^{\alpha}$

## ElGamal cryptosystem/1

Common elements:

- $\mathcal{G}$: cyclic group;
- $g \in \mathcal{G}$, generator of $\mathcal{G}$.

Secret key:

- $\alpha \in \mathbb{N}$.

Public key:

- $g^{\alpha} \in \mathcal{G}$.

## ElGamal cryptosystem/2

Encoding:

- $M \in \mathcal{G}$ message to be transmitted;
- the sender computes a *random* $k \in \mathbb{N}$;
- the sender transmits the pair

$$(e, f) = (g^k, M(g^\alpha)^k) = (g^k, Mg^{k\alpha}).$$

Decoding:

- the receiver computes

$$d = e^\alpha = g^{k\alpha};$$

- the receiver recovers

$$fd^{(-1)} = Mg^{k\alpha}(g^{k\alpha})^{-1} = M.$$

## ElGamal cryptosystem/3

Requirements on $\mathcal{G}$:

- There is an efficient implementation of the group operation:

$$(x, \alpha) \mapsto x^{\alpha}; \qquad (M, x) \mapsto Mx;$$

- There is an efficient implementation of *inversion*:

$$d \mapsto d^{-1};$$

- The Discrete Logarithm Problem is hard to solve in $\mathcal{G}$.

## Massey–Omura cryptosystem/1

Common elements:

- $\mathcal{G}$: Abelian group.

Secret key:

- $e_A \in \mathbb{N}$ with $\gcd(e, |\mathcal{G}|) = 1$;
- $d_A \in \mathbb{N}$ such that $e_A d_A \equiv 1 \pmod{|\mathcal{G}|}$.

There is no public key.

## Massey–Omura cryptosystem/2

Operation:

- $P \in \mathcal{G}$: message to be sent from `A` to `B`.

1. $A$ computes and sends
$$P' = P^{e_A};$$

2. $B$ computes and sends back
$$P'' = P'^{e_B} = P^{e_A e_B};$$

3. $A$ computes and sends back
$$P''' = P''^{d_A} = P^{e_A d_A e_B} = P^{e_B}$$

4. $B$ recovers
$$P'''^{d_B} = P^{e_B d_B} = P.$$

## Massey–Omura cryptosystem/3

Requirements on $\mathcal{G}$:

- The order of $\mathcal{G}$ is known;
- There is an efficient implementation of the exponentiation in $\mathcal{G}$:

$$(x, \alpha) \mapsto x^{\alpha};$$

- The Discrete Logarithm Problem is hard to solve in $\mathcal{G}$.

## Exponentiation in groups

Given:

- $\mathcal{G}$ group
- $g \in \mathcal{G}$
- $\alpha \in \mathbb{N}$

Determine:

$$g^{\alpha}.$$

Trivial approach:

$$g^{\alpha} = \underbrace{g \cdots g}_{\alpha \text{ times}}.$$

## Square and multiply

1. If $\alpha = 0$, then return

$$1;$$

2. If $\alpha = 1$, then return

$$g;$$

3. If $\alpha = 2k$, then compute $h = g^2$ and return

$$h^k;$$

4. If $\alpha = 2k + 1$, then compute $h = g^2$ and return

$$g \cdot h^k.$$

## Elliptic curves/1

- **Elliptic curve** over $\mathbb{K}$:
  (birationally equivalnent to) non–singular cubic with *at least* one point

$$y^2 + ay = x^3 + bx^2 + cxy + dx + e.$$

- If $\mathrm{char}\mathbb{K} \neq 2, 3$,

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

  or (equivalent)

$$y^2 = x(x-1)(x-\lambda).$$

## Elliptic curves/2

**Elliptic curve** over $\mathrm{GF}(2^n)$:

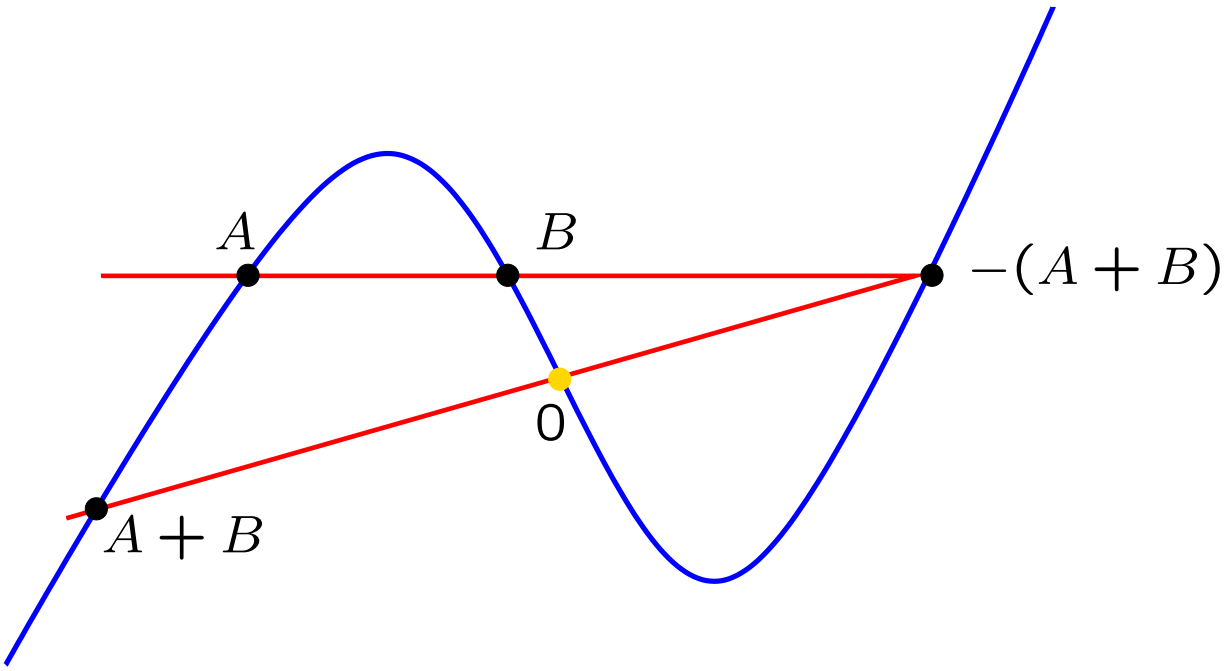
- non–supersingular

$$y^2 + xy = x^2 + ax^2 + b;$$

- supersingular ($2 = p \mid |\mathcal{C}|$)

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

## Elliptic curves/3:group law

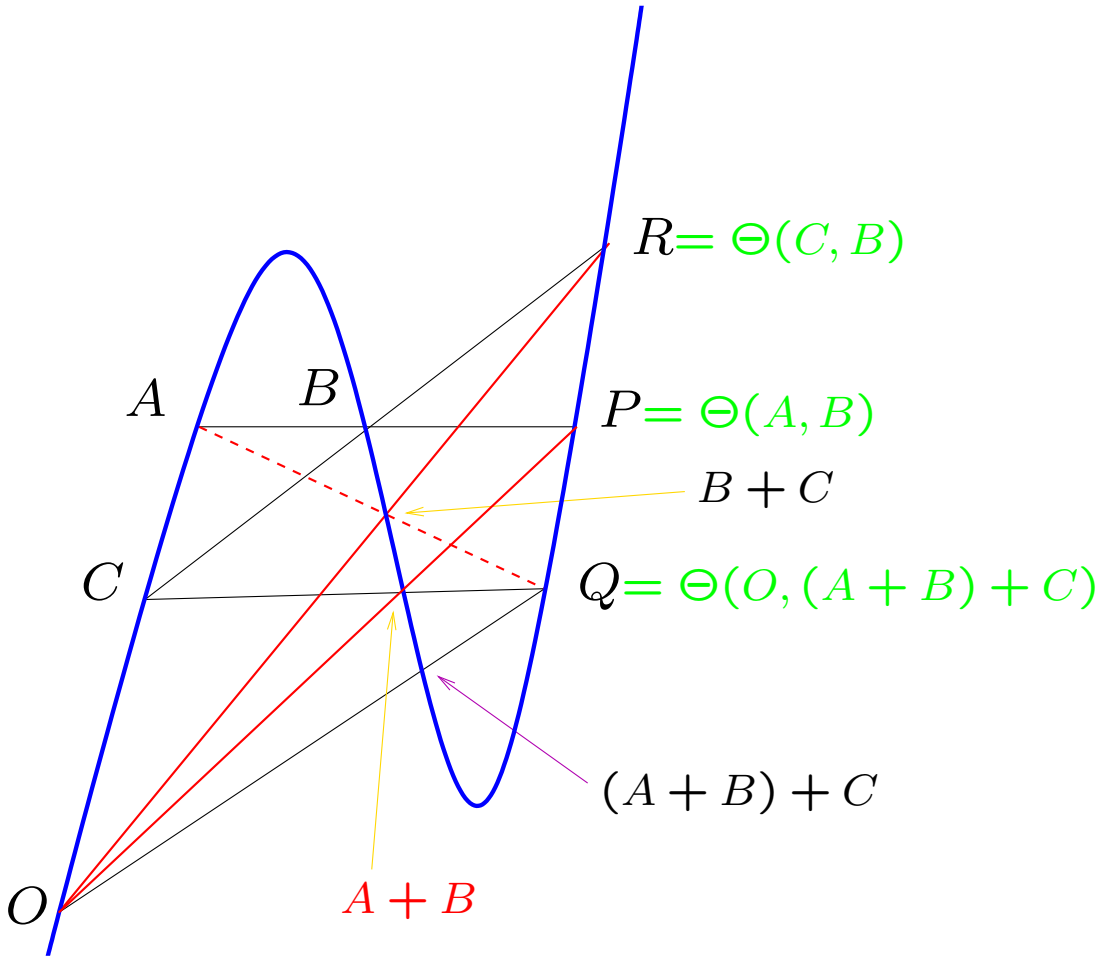


## Elliptic curves/4:group law

- $\mathcal{C}$ elliptic curve;
- $O \in \mathcal{C}$ fixed point (inflexion);
- $\ominus(A, B)$ third intersection of $AB$ with $\mathcal{C}$.

$$A + B := \ominus(\ominus(A, B), O).$$

## Elliptic curves/5:group law, associativity




Claim: $(B + C) \in AQ$.

$$\mathcal{K} : ABP + C(A + B)Q + O(B + C)R$$

## Elliptic curves/6:group law, inversion

- $O$ inflexion
- $P = (x, y) \in \mathcal{C}$
- $p \neq 2, 3$

$$P \mapsto -P = (-x, -y);$$

- $p = 2$, non–supersingular

$$P \mapsto -P = (x, y + x);$$

- $p = 2$, supersingular

$$P \mapsto -P = (x, y + c)$$

## Elliptic curves/7:group law, duplication, $p \neq 2, 3$

- $y^2 = x^3 + ax + b$;
- $P = (x_1, y_1)$;
- $2P = (x_3, y_3)$;
- $$\lambda = \frac{3x_1^2 + a}{2y_1}$$
- $x_3 = \lambda^2 - x_1 - x_2$;
- $y_3 = \lambda(x_1 - x_3) - y_1$.

## Elliptic curves/8:group law, sum, $p \neq 2, 3$

- $y^2 = x^3 + ax + b$;
- $P = (x_1, y_1)$;
- $Q = (x_2, y_2)$;
- $P + Q = (x_3, y_3)$;
- $$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
- $x_3 = \lambda^2 - x_1 - x_2$;
- $y_3 = \lambda(x_1 - x_3) - y_1$.

## Elliptic curves/9:group law, duplication, non–supersing.

- $y^2 + xy = x^3 + ax^2 + b$, $b \neq 0$;
- $P = (x_1, y_1)$;
- $2P = (x_3, y_3)$;
- $$\mu = x_1 + \frac{y_1}{x_1}$$
- $x_3 = \mu^2 + \mu + a$
- $y_3 = x_1^2 + (\mu + 1)x_3$

## Elliptic curves/10:group law, sum, non–supersing.

- $y^2 + xy = x^2 + ax^2 + b$, $b \neq 0$;
- $P = (x_1, y_1)$;
- $Q = (x_2, y_2)$;
- $P + Q = (x_3, y_3)$;
- $$\kappa = \frac{y_1 + y_2}{x_1 + x_2};$$
- $x_3 = \kappa^2 + \kappa + x_1 + x_2 + a$;
- $y_3 = \kappa(x_1 + x_3) + x_3 + y_1$.

Elliptic curves/11:group law, duplication, supersing.

- $y^2 + cx = x^3 + ax + b$, $c \neq 0$;
- $P = (x_1, y_1)$;
- $2P = (x_3, y_3)$;
- $$\eta = \frac{x_1^2 + a}{c}$$
- $x_3 = \eta^2$
- $y_3 = \eta(x_1 + x_3) + y_1 + c$

## Elliptic curves/12:group law, sum, supersing.

- $y^2 + cx = x^3 + ax + b$, $c \neq 0$;
- $P = (x_1, y_1)$;
- $Q = (x_2, y_2)$;
- $P + Q = (x_3, y_3)$;
- $$\kappa = \frac{y_1 + y_2}{x_1 + x_2};$$
- $x_3 = \kappa^2 + \kappa + x_1 + x_2$;
- $y_3 = \kappa(x_1 + x_3) + y_1 + c$.

## Elliptic curves/13:group order

- $|\mathcal{C}| = q + 1 - t$ with $|t| \leq 2\sqrt{q}$.

- $\mathbb{K} = \mathsf{GF}(p)$, $p \neq 2, 3$:

$$p + \sum_{x \in \mathbb{K}} \left( \frac{x^3 + ax + b}{p} \right),$$

  where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol;

- $\mathcal{C}$ non–supersingular, $\mathbb{K} = \mathsf{GF}(2^m)$:

$$2^m + 1 + (-1)^{\mathsf{Tr}(a)} \sum_{0 \neq x \in \mathbb{K}} (-1)^{\mathsf{Tr}(x + bx^{-2})};$$

- $\mathcal{C}$ supersingular, $\mathbb{K} = \mathsf{GF}(2^m)$:

$$2^m + 1 + (-1)^{\mathsf{Tr}(c^{-2}b)} \sum_{x \in \mathbb{K}} (-1)^{\mathsf{Tr}[c^{-2}(x^3 + ax)]}.$$

## Elliptic curves/14:group structure

Either:

- $\mathcal{C} = \mathbb{Z}_n$ or
- $\mathcal{C} = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with

  $n_2 \mid n_1$ and $n_2 \mid (q-1)$.

If $\mathcal{C}$ is square–free, then the group is cyclic.