# An overview about elliptic curve cryptosystems and pairings

Dutto Simone

Ph.D. Student in Pure and Applied Mathematics
Università degli Studi di Torino & Politecnico di Torino

*De Cifris AugustæTaurinorum* - 18 Aprile 2019

# Introduction
## Elliptic-Curve Cryptography

Elliptic-Curve Cryptography (ECC):

- was suggested in 1985 by Koblitz [1] and Miller [2];
- has same security level with smaller parameters than those required in Finite-Field Cryptography (e.g. DSA) and Integer-Factorization Cryptography (e.g. RSA).

# Pairing-Based Cryptography

Pairing-Based Cryptography (PBC):

- in the 1990s was exploited to break ECC [3];
- enables many elegant solutions to cryptographic problems and allows innovative protocols (three-party one-round key agreement [4], identity-base encryption [5], short signatures [6], . . . ).

# Diffie-Hellman Problem

ECC and PBC are approaches to Public-Key Cryptography (PKC) whose security is based on the:

**Diffie-Hellman Problem (DHP) [7]**

Given the cyclic group $G = \langle g \rangle$ and the elements $g^a, g^b \in G$, what is the value of $g^{ab}$?

This problem is assumed to be hard (Diffie-Hellman assumption) and the most efficient way to solve it is to solve the Discrete Logarithm Problem (DLP).

# Elliptic-Curve Cryptography

## Elliptic Curves

### Elliptic Curve

An elliptic curve $E$ over a field $\mathbb{k}$ (written $E/\mathbb{k}$) is a non-singular plane cubic defined by an (affine) equation $f(x, y) = 0$ with coefficients in $\mathbb{k}$.

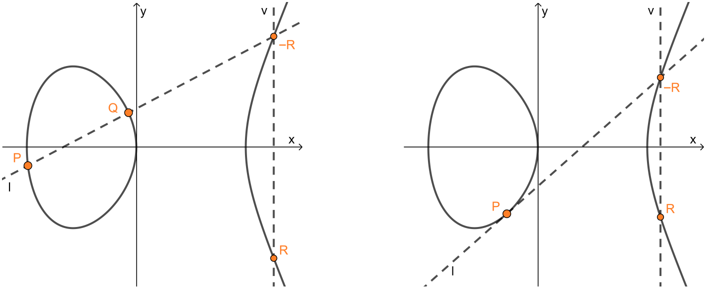
If $\mathrm{char}(\mathbb{k}) \notin \{2, 3\}$, by an appropriate change of variables, the curve equation can be written in its *short Weierstrass form*:

$$y^2 = x^3 + ax + b \quad (a, b \in \mathbb{k}).$$

# Group Definition

The group $E(\mathbb{F}_q)$ consists of all the points of the curve with coordinates $(x, y)$ over the algebraic closure of the finite field $\mathbb{F}_q$, in addition to the *point at infinity* $\mathcal{O}$.

The group law is the operation defined as follows:




$P + Q = R$ $\qquad$ $P + P = [2]P = R$

# Explicit Group Law

If $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ and $R = P + Q$, then the line joining them is $l : y = \lambda x + \nu$ where:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{and} \quad \nu = \frac{y_Q x_P - y_P x_Q}{x_P - x_Q}.$$

Thus, $x_R = x_{-R}$ is obtained from the equation of $l \cap E$:

$$(x - x_P)(x - x_Q)(x - x_R) = x^3 + ax + b - (\lambda x + \nu)^2$$

as the coefficient of $x^2$ while $y_R = -y_{-R}$ from the line $l$, so that:

$$x_R = \lambda^2 - x_P - x_Q \quad \text{and} \quad y_R = -(\lambda x_R + \nu).$$

If $P = (x_P, y_P)$ and $R = P + P = [2]P$, then the derivative in $x$ of the equation of $E$ is needed:

$$\frac{d(y^2)}{dy}\frac{dy}{dx} = \frac{d(x^3 + ax + b)}{dx} \Rightarrow \frac{dy}{dx} = \frac{3x^2 + a}{2y}\,.$$

Thus, the tangent to $E$ in $P$ is $l : y = \lambda x + \nu$ where:

$$\lambda = \frac{dy}{dx}(P) = \frac{3x_P^2 + a}{2y_P} \quad \text{and} \quad \nu = y_P - \lambda x_P\,.$$

As before, $x_R = x_{-R}$ is obtained from the equation of $l \cap E$ as the coefficient of $x^2$ (now with double $x_P$), while $y_R = -y_{-R}$ from the line $l$, so that:

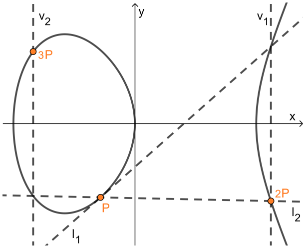
$$x_R = \lambda^2 - 2x_P \quad \text{and} \quad y_R = -(\lambda x_R + \nu)\,.$$

# Multiplication

Multiply points by integers is crucial in ECC, as it is the one-way operation that buries the DLP in $E(\mathbb{F}_q)$.

An efficient way to compute $R = [m]P$ is the *double-and-add* algorithm:

1. $m = (m_{n+1}, \ldots, m_1) \in \mathbb{Z}_2^{n+1}$
2. $R = P$
3. for $i \in \{n, \ldots, 1\}$
4. $\quad R = [2]R$
5. $\quad$ if $m_i = 1$
6. $\quad\quad R = R + P$




In general, this algorithm will take $log_2 m$ doublings and roughly half as many additions to compute $[m]P$.

# Speeding Up Computations

Computations in ECC are more complicated than those in other DLP based protocols (e.g., with $\mathbb{F}_q^*$).

The more abstract nature of elliptic curve groups can be a benefit: best available attacks remain generic.

In order to speed up computations:

- projective coordinates are preferred to affine ones, since no inversion in $\mathbb{F}_q$ is required;
- if some conditions hold, some equation forms different from Weierstrass can be advantageous (e.g., *Jacobi-quartic* [8]).

# Structure of $E(\mathbb{F}_q)$

## Proposition [9](5.78)

$E(\mathbb{F}_q)$ is either a cyclic group or isomorphic to a product of two cyclic groups $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_1 | n_2$.

In ECC, it is preferred the former case, or at least for $n_1$ to be very small.

In addition, the group order $\#E(\mathbb{F}_q)$ must be as close to prime as possible. This is because the complexity of the DLP is dependent on the size of the largest prime subgroup of $E(\mathbb{F}_q)$.

# Point Counting

**Theorem (Hasse Bound) [10]**

$\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

$t$ is called the *trace of Frobenius*, because of the *Frobenius endomorphism* $\pi : E \to E, (x, y) \mapsto (x^q, y^q)$ and its characteristic polynomial $\pi^2 - [t] \circ \pi + [q] = 0$.

**Theorem (Deuring) [11]**

If $q$ is prime, then $\forall N \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ $\exists E \mid N = \#E(\mathbb{F}_q)$.

Shoof's polynomial-time algorithm ($O(\log^8 q)$) for $t$ [12]:

- solve $(x^{q^2}, y^{q^2}) - [t_l](x^q, y^q) + [q_l](x, y) = \mathcal{O}$ for $t_l \equiv t (\bmod\ l)$ where $q_l \equiv q (\bmod\ l)$ and $(x, y) \in \{P \in E \mid [l]P = \mathcal{O}\}$ (*l-torsion group*).

  Unfortunately, $l$-torsion points cannot be explicitly used, since it is unknown where they are defined (it depends on the unknown group order).

  However, the equation can be restricted to $R_l = \mathbb{F}_q[x, y]/\langle \psi_l(x), y^2 - (x^3 + ax + b) \rangle$ where $\psi_l(x)$ is a *division polynomial* (whose roots are the $x$-coordinates of the $l$-torsion points) [13];
- when $\prod_l l \geq 4\sqrt{q}$, $t$ can be found through CRT.

# Example [14](2.2.10)

$E/\mathbb{F}_{13} : y^2 = x^3 + 2x + 1$

$\#E(\mathbb{F}_{13}) = q + 1 - t$ , where $|t| \le 2\sqrt{13} \cong 7$

Schoof: $\prod_l l \ge 4\sqrt{q} \cong 15 \Rightarrow l \in \{3, 5\}$.

- $l = 3 : \psi_3(x) = 3x^4 + 12x^2 + 12x + 9, q_3 = 1$.
  After computing $(x^{169}, y^{169}), (x^{13}, y^{13})$ and $[q_3](x, y)$ in $R_3 = \mathbb{F}_q[x, y]/\langle\psi_3(x), y^2 - (x^3 + 2x + 1)\rangle$ and testing incremental $t_3$ until the Frobenius polynomial in $R_3$ is satisfied, $t_3 = 0$ is obtained.
- $l = 5$ : analogously, $t_5 = 1$ is obtained.

The CRT with $t \equiv 0(\mathrm{mod} 3), t \equiv 1(\mathrm{mod} 5)$ and $|t| \le 7$ gives $t = 6$ so that $\#E(\mathbb{F}_{13}) = 13 + 1 - 6 = 8$.

$E(\mathbb{F}_{13})=\{\mathcal{O},(0,1),(0,12),(1,2),(1,11),(2,0),(8,3),(8,10)\}$ and one of its generators is $(0,1)$. So if $A$ and $B$ want to share a secret, they can take $P=(0,1)$ as basis and:

- $A$ chooses $a=5$ and sends to $B$
  $R=[a]P=[5](0,1)=[(101)_2](0,1)$:
  after initializing $R=P=(0,1)$,
  $a_2=0 \Rightarrow R=[2]R=(1,11)$,
  $a_1=1 \Rightarrow R=[2]R+P=(2,0)+(0,1)=(8,3)$;
- $B$ does the same with $b=3$ and sends $[b]P=[3](0,1)=(8,10)$ to $A$;
- $A$ can evaluate $[a]([b]P)=[5](8,10)=(0,12)$;
- $B$ can evaluate $[b]([a]P)=[3](8,3)=(0,12)$.

# Pairings-Based Cryptography

## Divisors

### Divisors

A divisor on an elliptic curve $E$ is $D = \sum_{P \in E} n_P(P)$, where all but finitely many $n_P \in \mathbb{Z}$ are zero.

The set of all divisors of $E$ is $\mathrm{Div}(E)$ and is a group with natural addition and identity $0 = \sum_{P \in E} 0(P)$.

The degree of a divisor is $\mathrm{Deg}(D) = \sum_{P \in E} n_P$ and its support is $\mathrm{supp}(D) = \{P \in E \mid n_P \neq 0\}$.

The divisor of a function $f$ is $(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$. $\mathrm{Deg}((f)) = 0$, $(fg) = (f) + (g)$, $(f) = 0$ iff $f$ constant.

# Divisor Class Group

Divisors with degree zero form a subgroup written as $\mathrm{Div}^0(E) \subset \mathrm{Div}(E)$.

A *principal* divisor is $D$ for which $\exists f \mid D = (f)$ and they form the subgroup $\mathrm{Prin}(E) \subset \mathrm{Div}^0(E) \subset \mathrm{Div}(E)$.

**Theorem [15](IX.2)**

$D = \sum_P n_P(P) \in \mathrm{Div}^0(E)$ is principal iff $\sum_P [n_P]P = \mathcal{O}$.

$D_1, D_2 \in \mathrm{Div}(E)$ are called *equivalent* ($D_1 \sim D_2$) if $\exists f \mid D_1 = D_2 + (f)$ (i.e., $D_1 - D_2 \in \mathrm{Prin}(E)$).

The *divisor class group*, or *Picard group*, of $E$ is

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E) .$$

The *Riemann-Roch theorem* [13](II.5.5) implies:

**Proposition [13](III.3.4)**

- For any divisor $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ satisfying $D \sim (P) - (\mathcal{O})$.
- The map $\sigma : \mathrm{Div}^0(E) \to E, D \mapsto P$ is surjective.
- $\sigma(D_1) = \sigma(D_2)$ iff $D_1 \sim D_2$.

Thus, $\sigma$ induces an isomorphism between $\mathrm{Pic}^0(E)$ and $E$.

In PBC, elliptic curves are preferred because of this property that makes their computational speed unrivaled.

# Weil Reciprocity

The evaluation of a function $f$ at $D = \sum_{P \in E} n_P(P)$, where $(f)$ and $D$ have disjoint supports, is

$$f(D) = \prod_{P \in E} f(P)^{n_P} .$$

If $P \in \text{supp}((f)) \cap \text{supp}(D)$, then $P$ is a zero or pole of $f$ and $f(P)^{n_P}$ would be 0 or $\infty$.

**Theorem (Weil Reciprocity) [15](IX.3)**

If $f, g$ are non-zero functions such that $(f)$ and $(g)$ have disjoint supports, then $f((g)) = g((f))$.

# Pairings

## Pairing (in cryptography)

A *pairing* is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ between finite abelian groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, which is:

- *bilinear*, i.e., $\forall P, P' \in \mathbb{G}_1, Q, Q' \in \mathbb{G}_2$
$$e(P + P', Q) = e(P, Q) \cdot e(P', Q)\,,$$
$$e(P, Q + Q') = e(P, Q) \cdot e(P, Q')\,;$$
- *non-degenerate*, i.e., $\forall P \in \mathbb{G}_1 \, \exists Q \in \mathbb{G}_2 \,|\, e(P, Q) \neq 1$ and $\forall Q \in \mathbb{G}_2 \, \exists P \in \mathbb{G}_1 \,|\, e(P, Q) \neq 1$;
- *efficiently computable* and *hardly invertible*.

In particular, $e([a]P, [b]Q) = e(P, Q)^{ab}$ (DLP).

# $r$-torsion

For the only known admissible pairings (Weil and Tate), $P$ and $Q$ must come from disjoint cyclic subgroups of same prime order $r$ (because of the *Weil reciprocity*).

Thus, an important group is the *r-torsion* of $E/\mathbb{k}$:

$$E[r] = \{P \in E \mid [r]P = \mathcal{O}\}.$$

**Theorem [9](13.13)**

If $\mathrm{char}(\mathbb{k}) = p$ with $p = 0$ or $p \nmid r$, then $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$.

$\#E[r] = r^2$ and, since $\mathcal{O}$ belongs to all its subgroups, $E[r]$ consists of $r+1$ cyclic subgroups of order $r$.

# Embedding degree

When $E(\mathbb{F}_q)$ contains only one subgroup of order $r$, $\mathbb{F}_q$ can be extended to $\mathbb{F}_{q^k}$ such that $E(\mathbb{F}_{q^k})$ contains at least one other subgroup of order $r$.

The integer $k > 1$ is called *embedding degree*, and can be found as the smallest positive integer such that:

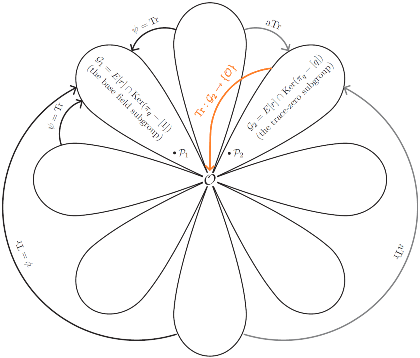
- $r \mid (q^k - 1)$;
- $\mathbb{F}_{q^k}$ contains all the $r$-roots of unity in $\overline{\mathbb{F}}_q$;
- $E[r] \subset E(\mathbb{F}_{q^k})$ [13](XI.6.2).

The focus will be on $r \mid \#E(\mathbb{F}_q)$ but $r^2 \nmid \#E(\mathbb{F}_q)$, so that the $r$-torsion subgroup in $E(\mathbb{F}_q)$ is unique and $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$ that contains all $E[r]$.

# Characterization of $E[r]$

$E[r] \cap E(\mathbb{F}_q)$ is called the *base-field* subgroup $\mathcal{G}_1$.
$\pi$ acts trivially on $\mathcal{G}_1$, so that it can be defined as
$\mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$.

The other eigenvalue of $\pi$ is $q$ and it defines $\mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$, called the *trace-zero* subgroup because $\forall P \in \mathcal{G}_2$ $\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \pi^i(P) = \mathcal{O}$.




The *trace* sends all other subgroups in $\mathcal{G}_1$, while they are mapped to $\mathcal{G}_2$ by the *anti-trace* $\mathrm{aTr}(P) = [k]P - \mathrm{Tr}(P)$.

# Supersingular Curves

## Supersingular curve

An elliptic curve $E$ is called *supersingular* if $\#E(\mathbb{F}_q) = q + 1$.

For supersingular curves only, there exists a non-$\mathbb{F}_q$-rational map $\phi$ that takes points in $E(\mathbb{F}_q)$ to points in $E(\mathbb{F}_{q^k})$, called *distortion map*.

In particular, $\phi$ maps out of $\mathcal{G}_1$ and $\mathcal{G}_2$ in different subgroups of $E[r]$.

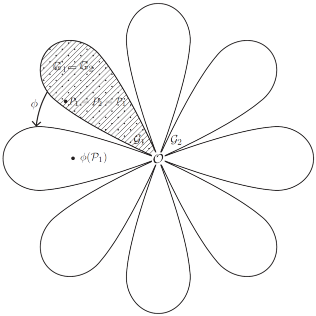
# Pairing Types

Usually, $\mathbb{G}_T = \mathbb{F}^*_{q^k}, \mathbb{G}_1 = \mathcal{G}_1$ and the choice of $\mathbb{G}_2$ among the subgroups of $E[r]$ divides pairings in 4 types [16].

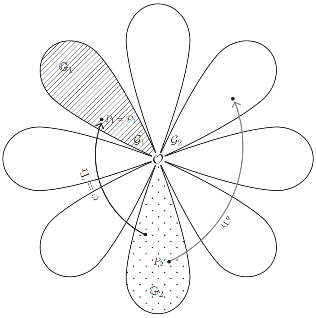
The main factors affecting the classification are:

- the ability to hash or sample elements of $\mathbb{G}_2$;
- the existence of a $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ (that makes security proofs work);
- computation efficiency.

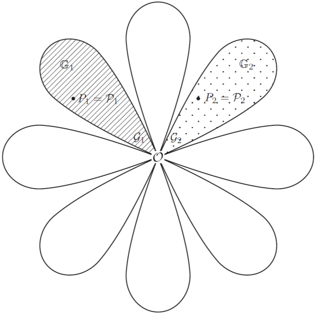
1. $E$ supersingular, $\mathbb{G}_2 = \mathcal{G}_1$ and $e(P, Q) = \hat{e}(P, \phi(Q))$ ($\hat{e}$ Weil or Tate pairing).
   Pros: no hashing problems, trivial $\psi$.
   Cons: supersingularity affects computation efficiency.



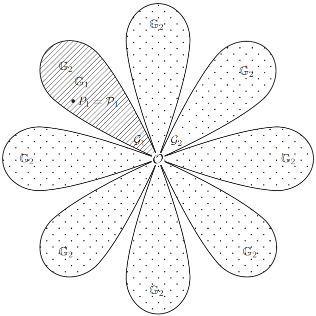
1. $E$ supersingular, $\mathbb{G}_2 = \mathcal{G}_1$ and $e(P, Q) = \hat{e}(P, \phi(Q))$ ($\hat{e}$ Weil or Tate pairing).
   Pros: no hashing problems, trivial $\psi$.
   Cons: supersingularity affects computation efficiency.
2. $E$ ordinary, $\mathbb{G}_2 \subset E[r], \mathbb{G}_2 \neq \mathcal{G}_1, \mathcal{G}_2$.
   Pros: $\psi = \mathrm{Tr}$, $\mathrm{aTr} : \mathbb{G}_2 \to \mathcal{G}_2$ helps in computation.
   Cons: no efficient way to hash.



1. $E$ supersingular, $\mathbb{G}_2 = \mathcal{G}_1$ and $e(P, Q) = \hat{e}(P, \phi(Q))$ ($\hat{e}$ Weil or Tate pairing).
   Pros: no hashing problems, trivial $\psi$.
   Cons: supersingularity affects computation efficiency.
2. $E$ ordinary, $\mathbb{G}_2 \subset E[r], \mathbb{G}_2 \neq \mathcal{G}_1, \mathcal{G}_2$.
   Pros: $\psi = \mathrm{Tr}$, $\mathrm{aTr} : \mathbb{G}_2 \to \mathcal{G}_2$ helps in computation.
   Cons: no efficient way to hash.
3. $E$ ordinary, $\mathbb{G}_2 = \mathcal{G}_2$.
   Pros: good hash and computation.
   Cons: $\psi : \mathcal{G}_2 \to \mathcal{G}_1$ not efficient.



1. $E$ supersingular, $\mathbb{G}_2 = \mathcal{G}_1$ and $e(P, Q) = \hat{e}(P, \phi(Q))$ ($\hat{e}$ Weil or Tate pairing).
   Pros: no hashing problems, trivial $\psi$.
   Cons: supersingularity affects computation efficiency.
2. $E$ ordinary, $\mathbb{G}_2 \subset E[r], \mathbb{G}_2 \neq \mathcal{G}_1, \mathcal{G}_2$.
   Pros: $\psi = \mathrm{Tr}$, $\mathrm{aTr} : \mathbb{G}_2 \to \mathcal{G}_2$ helps in computation.
   Cons: no efficient way to hash.
3. $E$ ordinary, $\mathbb{G}_2 = \mathcal{G}_2$.
   Pros: good hash and computation.
   Cons: $\psi : \mathcal{G}_2 \to \mathcal{G}_1$ not efficient.
4. $E$ ordinary, $\mathbb{G}_2 = E[r]$.
   Pros: $\psi = \mathrm{Tr}$, efficient computation.
   Cons: no efficient way to hash ($\mathbb{G}_2$ is not cyclic and of order $r^2$).



# Weil and Tate pairings

Both pairings exploit that, from Th.[15](IX.2), for any $m \in \mathbb{Z}$, $P \in E$, there exists a function $f_{m,P}$ with divisor:

$$(f_{m,P}) = m(P) - ([m]P) - (m-1)(\mathcal{O}),$$

where, for $m = 0$, $f_{0,P} = 1$ and $(f_{0,P}) = 0$.

If $P \in E[r]$ then $(f_{r,P}) = r(P) - r(\mathcal{O})$.

$(f_{m+1,P}) - (f_{m,P}) = (P) + ([m]P) - ([m+1]P) - (\mathcal{O})$ which is the divisor of $l_{[m]P,P}/v_{[m+1]P}$ (lines used in the points addition), so that:

$$f_{m+1,P} = f_{m,P}\frac{l_{[m]P,P}}{v_{[m+1]P}}.$$

## Weil Pairing [17]

Let $P, Q \in E(\mathbb{F}_{q^k})[r]$ and $D_P, D_Q \in \mathrm{Div}^0(E)$ with disjoint supports such that $D_P \sim (P) - (\mathcal{O})$ and $D_Q \sim (Q) - (\mathcal{O})$. There exist function $f$ and $g$ such that $(f) = rD_P$ and $(g) = rD_Q$, and the *Weil pairing* is:

$$w_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \to \mu_r\,,\ (P, Q) \mapsto \frac{f(D_Q)}{g(D_P)}\,.$$

$f_{r,P}$ and $f_{r,Q}$ can not be used as $f$ and $g$ because both $(f_{r,P})$ and $(f_{r,Q})$ contains $\mathcal{O}$, but if $R, S \in E(\mathbb{F}_{q^k})$ then $D_P = (P + R) - (R)$ and $D_Q = (Q + S) - (S)$ can be considered, so that $f = f_{r,P}/(l_{P,R}/v_{P+R})^r$ and $g = f_{r,Q}/(l_{Q,S}/v_{Q+S})^r$ have $(f) = rD_P$ and $(g) = rD_Q$.

Given the *coset* $rE(\mathbb{F}_{q^k}) = \{[r]P \mid P \in E(\mathbb{F}_{q^k})\}$, $E(\mathbb{F}_{q^k})[r]$ represents $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$.

## Tate Pairing [18]

Let $P \in E(\mathbb{F}_{q^k})$, $f \mid (f) = r(P) - r(\mathcal{O})$, $Q \in E(\mathbb{F}_{q^k})$ representative of a class in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ and $D_Q \in \mathrm{Div}^0(E) \mid D_Q \sim (Q) - (\mathcal{O})$ whose support is disjoint to that of $(f)$. The *Tate pairing* is:

$$t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r\,,$$
$$(P, Q) \mapsto f(D_Q)\,.$$

$f$ can be $f_{r,P}$ while $D_Q$ can be taken as $(Q + R) - (R)$, where $R \in E(\mathbb{F}_{q^k})$.

Outputs of Tate pairing lie in equivalence classes, while unique values are preferred. Thus an update is required.

## Reduced Tate Pairing

Given $P, f, Q, D_Q$ as before, the *reduced Tate pairing* is:

$$T_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r \, ,$$
$$(P, Q) \mapsto t_r(P, Q)^{\#\mathbb{F}_{q^k}/r} = f(D_Q)^{(q^k-1)/r} \, .$$

It is possible to consider $P \in \mathcal{G}_1$ and $Q \in \mathcal{G}_2$ (Type 3 pairing), since every value in $\mu_r$ will still be reached.

# Miller's Algorithm

In order to compute $w_r(P, Q)$ and $T_r(P, Q)$, the evaluation of $f_{r,P}(D_Q)$ is required.

The difference between $(f_{r,P}) = r(P) - r(\mathcal{O})$ and $(f_{r-1,P}) = (r-1)(P) - ([r-1]P) - (r-2)(\mathcal{O})$ is $(P) + ([r-1]P) - 2(\mathcal{O})$, which corresponds to a multiplication by $v_{[r-1]P}$, so that $f_{r,P} = v_{[r-1]P} f_{r-1,P}$ and:

$$f_{r,P} = v_{[r-1]P} \prod_{i=1}^{r-1} \frac{l_{[i]P,P}}{v_{[i+1]P}} = l_{[r-1]P,P} \prod_{i=1}^{r-2} \frac{l_{[i]P,P}}{v_{[i+1]P}}$$

Thus, this method has exponential complexity $O(r)$ and, for huge $r$, it is unfeasible.

Miller's algorithm [19] makes pairings practical.

The idea is to observe that the difference between $(f_{2m,P}) = 2m(P) - ([2m]P) - (2m-1)(\mathcal{O})$ and $(f^2_{m,P}) = 2m(P) - 2([m]P) - 2(m-1)(\mathcal{O})$ is $2([m]P) - ([2m]P) - (\mathcal{O})$, which corresponds to the quotient of $l_{[m]P,[m]P}$ and $v_{[2m]P}$, so that:

$$f_{2m,P} = f^2_{m,P} \cdot \frac{l_{[m]P,[m]P}}{v_{[2m]P}} .$$

This gives rise to a *double-and-add* algorithm with polynomial complexity $O(\log r)$.

Finally, since $f_{m,P}$ becomes too large to store and only $f_{r,P}(D_Q)$ is required, at each step $f_{m,P}(D_Q)$ is evaluated.

# Pairing-Friendly Curves

Solving the DLP in $\mathbb{G}_1$, $\mathbb{G}_2$ or $\mathbb{G}_T$ can broke the system. Thus, the attack complexity is the minimum between the size of $r$ (for $\mathbb{G}_1$, $\mathbb{G}_2$) and that of $q^k$ (for $\mathbb{G}_T$) and can be described by $k \cdot \rho = k \cdot \frac{\log q}{\log r}$. Since $r \mid \#E(\mathbb{F}_q), \rho \geq 1$.

In addition, the pairing must be efficient, which means that arithmetic in $\mathbb{F}_{q^k}$ must be fast, i.e., $k$ must be small.

To sum up, a curve is *pairing-friendly* [20] if:

- there is a prime $r \geq \sqrt{q}$ (i.e. $\rho \leq 2$);
- the embedding degree $k$ is less than $\log_2(r)/8$.

# Example [14](5.3.1)

$E/\mathbb{F}_q : y^2 = x^3 + 21x + 15$ with $q = 47$ and $\#E(\mathbb{F}_q) = 51 = 3 \cdot 17$, so $r = 17$ and $\rho \cong 1.36$. Since $17 \mid (47^4 - 1)$, $k = 4$ and $\mathbb{F}_{q^4} = \mathbb{F}_q(u)$ where $u^4 - 4u^2 + 5 = 0$.

$P = (45, 23)$ has order 17 in $E(\mathbb{F}_q)$, thus $P \in \mathcal{G}_1$.

$Q \in \mathcal{G}_2$ can be found from any $R \in E(\mathbb{F}_{q^4})$ by multiplying it for $h = 3^3 \cdot 5^4$ (since $\#E(\mathbb{F}_{q^4}) = 3^3 \cdot 5^4 \cdot 17^2$), so that $[h]R \in E[17]$ and $\mathrm{aTr}([h]R) \in \mathcal{G}_2$.
For example, $Q = (31u^2 + 29, 35u^3 + 11u) \in \mathcal{G}_2$.

Chosen $D_P = ([2]P) - (P)$ and $D_Q = ([2]Q) - (Q)$,
$T_r$ requires only $f_{r,P}(D_Q)$ while $w_r$ requires also $f_{r,Q}(D_P)$.

Miller: $r = (1001)_2$ and the steps are:

| $r_i$ | $R$ | $l/v$ | $l(D_Q)/v(D_Q)$ | $f_{r,P}(D_Q)$ |
|---|---|---|---|---|
| 1 | (45,23) | | | 1 |
| 0 | (12,16) | $\frac{y+33x+43}{x+35}$ | $41u^3+32u^2+2u+21$ | $41u^3+32u^2+2u+21$ |
| 0 | (27,14) | $\frac{y+2x+7}{x+20}$ | $4u^3+5u^2+28u+17$ | $22u^3+27u^2+30u+33$ |
| 0 | (18,31) | $\frac{y+42x+27}{x+29}$ | $6u^3+13u^2+33u+28$ | $36u^3+2u^2+21u+37$ |
| 1 | (45,24) | $\frac{y+9x+42}{x+2}$ | $46u^3+45u^2+u+20$ | $10u^3+21u^2+40u+25$ |
| | $\mathcal{O}$ | $x+2$ | $6u^2+43$ | $17u^3+6u^2+10u+22$ |

$T_r(P,Q) = f_{r,P}(D_Q)^{(q^k-1)/r} = 33u^3 + 43u^2 + 45u + 39$,
for $w_r(P,Q)$ the calculations are analogous.

# Joux's protocol [4]

If $A$, $B$ and $C$ want to share a secret, they can choose a common $P \in \mathcal{G}_1$ for a pairing of Type 1 $e(P, P)$ and three personal elements $a, b, c \in \mathbb{F}_q^*$, then:

- $A$ sends $[a]P$ to $B$ and $C$;
- $B$ sends $[b]P$ to $A$ and $C$;
- $C$ sends $[c]P$ to $A$ and $B$;
- $A$ evaluates $e([b]P, [c]P)^a$;
- $B$ evaluates $e([a]P, [c]P)^b$;
- $C$ evaluates $e([a]P, [b]P)^c$.

Now they share the secret $K = e(P, P)^{abc}$.

# The future menace

Quantum computers, thanks to the Shor's algorithm, are theoretically capable of break DLP-based cryptography.

# Bibliography I

[1] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, vol. 48, no. 177, 1987.

[2] V. S. Miller, “Use of elliptic curves in cryptography,” in *Advances in Cryptology - CRYPTO '85 Proceedings*, 1986.

[3] A. Menezes, S. Vanstone, and T. Okamoto, “Reducing elliptic curve logarithms to logarithms in a finite field,” in *Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*, 1991.

[4] A. Joux, “A one round protocol for tripartite diffie-hellman,” in *Algorithmic Number Theory*, 2000.

[5] D. Boneh and M. K. Franklin, “Identity-based encryption from the weil pairing,” in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, 2001.

[6] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in *Advances in Cryptology - ASIACRYPT 2001*, 2001.

[7] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. on Information Theory*, vol. 22, no. 6, 1976.

# Bibliography II


[8] O. Billet and M. Joye, "The jacobi model of an elliptic curve and side-channel analysis," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 2003.

[9] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *The Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. Chapman & Hall/CRC, 2012.

[10] H. Hasse, "Zur theorie der abstrakten elliptischen funktionenkörper I, II & III," *Journal für die reine und angewandte Mathematik*, vol. 175, 1936.

[11] M. Deuring, "Die typen der multiplikatorenringe elliptischer funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 14, no. 1, 1941.

[12] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Mathematics of Computation*, vol. 44, no. 170, 1985.

[13] J. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[14] C. Costello, "Pairings for beginners," 2012.

# Bibliography III

[15] I. Blake, G. Seroussi, and N. Smart, *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*.
Cambridge University Press, 2005.

[16] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, no. 16, 2008.

[17] A. Weil, "Sur les fonctions algébriques à corps de constantes fini," *Les Comptes rendus de l'Académie des sciences*, vol. 210, 1940.

[18] J. Tate, "WC-groups over $p$-adic fields," in *Séminaire Bourbaki: années 1956/57 - 1957/58, exposés 137-168*, 1958.

[19] V. S. Miller, "The weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, no. 4, 2004.

[20] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," *Journal of Cryptology*, vol. 23, no. 2, 2010.