

# Crypto Engineering

## ECC

2019-11-08

In these exercises, we will study two simple cryptanalytic applications of elliptic curve pairings. We first give some definitions.

Let  $E/\mathbb{F}_q$  be an elliptic curve defined over  $\mathbb{F}_q$ ,  $P, Q, S, T \in E$ .

- Let  $r$  be a positive integer. If  $[r]P = O$ , then we say that  $P$  is an  $r$ -torsion point of  $E$ .
- The set of all  $r$ -torsion points of  $E$  forms a subgroup of  $E(\overline{\mathbb{F}_q})$ , the  $r$ -torsion group  $E[r]$ .
- Let  $p := \text{char}(\mathbb{F}_q)$  (i.e.  $q = p^k$  for some prime  $p$ ), then if  $p \nmid r$ ,  $E[r] \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ . In all of the following, we will assume to be in this case.
- The *embedding degree* of  $r$  in  $\mathbb{F}_q$  is the smallest integer  $d$  s.t.  $E[r] \subseteq E(\mathbb{F}_{q^d})$ , or equivalently s.t.  $q^d \equiv 1 \pmod{r}$ , or  $\mu_r \subseteq \mathbb{F}_{q^d}^\times$  (where  $\mu_r$  denotes the group of  $r^{\text{th}}$  roots of unity).
- The *Weil pairing*  $e_r$  is a map  $E[r] \times E[r] \rightarrow \mu_r$  that in particular is bilinear ( $e_r(S, T \oplus Q) = e_r(S, T) e_r(S, Q)$ ;  $e_r(S \oplus Q, T) = e_r(S, T) e_r(Q, T)$ ), alternating ( $e_r(T, T) = 1$ ;  $e_r(T, S) = e_r(S, T)^{-1}$ ) and non-degenerate (if  $e_r(S, T) = 1$  for all  $S \in E[r]$ , then  $T = O$ ).
- Miller's algorithm (which uses a “double-and-add” strategy) allows to compute  $e_r(\cdot, \cdot)$  with  $O(\log(r))$  operations in  $\mathbb{F}_{q^d}$ .

### Exercise 0

Let  $P, Q \in E/\mathbb{F}_q$  have prime order  $r$ , and  $d$  be the embedding degree of  $r$  in  $\mathbb{F}_q$ .

Show that if  $Q \notin \langle P \rangle$ , then  $\langle P, Q \rangle = E[r]$  and  $\omega := e_r(P, Q)$  is a generator of  $\mu_r$ .

### Exercise 1: Solving (co-)DDHP on elliptic curves with small embedding degree [based on (Galbraith, *Mathematics of PKC*, Exercise 26.5.7)]

We reuse the notations of the previous exercise.

The DDHP asks that given  $(P, [a]P, [b]P, [x]P)$ , one must decide whether  $x \equiv ab \pmod{r}$  or  $x \xleftarrow{\$} [0, r-1]$ . The co-DDHP asks that given  $(P, [a]P, Q, [b]Q)$ , one must decide whether  $a \equiv b \pmod{r}$ .

**Q.1:** Show that if  $Q \in \langle P \rangle$ , then DDHP and co-DDHP are equivalent.

**Q.2:**

1. Show that if  $Q \notin \langle P \rangle$ , one can solve co-DDHP using the Weil pairing  $e_r$ .
2. Assuming that  $q$  has a “reasonable size” (e.g.  $\approx 256$  bits), under which condition on  $d$  will the attack be efficient? How does it relate to the hardness of the DLP in  $\langle P \rangle$  (assuming that  $P \in E(\mathbb{F}_q)$ )?
3. Why does a similar approach not work for DDHP?
4. Would this unsuccessful approach work if the pairing were not alternating?

REMARK. Some alternative pairings to the Weil pairing are sometimes non-alternating.

**Exercise 2: The Menezes-Okamoto-Vanstone attack on the elliptic curve DLP**

We reuse the notations of the previous exercise.

We wish to solve the DLP in  $\langle P \rangle$  w.r.t.  $P$ : given  $P, R := [k]P, k \in \llbracket 0, r-1 \rrbracket$ , find  $k$ .

**Q. 1:** Give an expression of  $e_r(R, Q) = e([k]P, Q)$  in function of  $k$  and  $\omega := e_r(P, Q)$ .

**Q. 2:** Using the previous expression, show how to retrieve  $k$  by solving a DLP in  $\mathbb{F}_{q^d}^\times$ .

**Q. 3:** Conclude on the importance of the embedding degree for the hardness of the DLP in  $\langle P \rangle$ .

**Note:** In most cases, this attack is not a concern, as the embedding degree is usually expected to be proportional to  $r$  (and its value can be easily computed). However, applications of *pairing-based* cryptography precisely require it to be “small enough” for the computations to be efficient, and one must be careful in how to choose the systems’ parameters to ensure the hardness of the DLP both in  $E$  and in  $\mathbb{F}_{q^d}$ .