Implementing Cryptographic Pairings at Standard Security Levels

Andreas Enge* and Jérôme Milan

1 INRIA, LFANT, CNRS, UMR 5251, Univ. Bordeaux, IMB, 33400 Talence, France
2 INRIA, CNRS, UMR 7161, École polytechnique, LIX, 91128 Palaiseau, France

Abstract. This study reports on an implementation of cryptographic pairings in a general purpose computer algebra system. For security levels equivalent to the different AES flavours, we exhibit suitable curves in parametric families and show that optimal ate and twisted ate pairings exist and can be efficiently evaluated. We provide a correct description of Miller’s algorithm for signed binary expansions such as the NAF and extend a recent variant due to Boxall et al. to addition-subtraction chains. We analyse and compare several algorithms proposed in the literature for the final exponentiation. Finally, we give recommendations on which curve and pairing to choose at each security level.

Keywords: elliptic curve cryptology, pairings, implementation.

1 Pairings on Elliptic Curves

In this article, we treat cryptographic bilinear pairings $G_1 \times G_2 \to G_T$ on elliptic curves $E$ defined over some finite field $\mathbb{F}_q$ of characteristic $p$. We emphasise that our aim is not to set new speed records for particular curves, cf. [2011], but to compare different choices of pairings and parameters at various security levels, using a general purpose, but reasonably optimised, implementation in a general purpose computer algebra system. Such an analysis will be meaningful assuming that the ratios between the various operations remain constant when switching to hand-optimised assembly implementations in each instance.

We fix the following standard notations and setting. Let $E(\mathbb{F}_q)$ denote the $\mathbb{F}_q$-rational points on $E$, and let $r$ be a prime divisor of $\#E(\mathbb{F}_q) = q + 1 - t$ that does not divide $q - 1$, where $t$ is the trace of Frobenius. Let the embedding degree $k$ be the smallest integer such that $r$ divides $q^k - 1$, and denote by $\pi$ the Frobenius map $E(\mathbb{F}_q^k) \to E(\mathbb{F}_q^k)$, $(x, y) \mapsto (x^q, y^q)$. The $r$-torsion subgroup $E[r]$ is defined over $\mathbb{F}_q^k$, and it contains the non-trivial subgroup $E(\mathbb{F}_q)[r]$ of $\mathbb{F}_q$-rational $r$-torsion points. Denote by $\mu_r$ the subgroup of $r$-th roots of unity in $\mathbb{F}_q^k$.

Typically, $G_T = \mu_r$, $G_1 = E(\mathbb{F}_q)[r]$, and $G_2$ is a subgroup of order $r$ of either $E[r]$ or of $E(\mathbb{F}_q^k)/rE(\mathbb{F}_q^k)$.

* This research was partially funded by ERC Starting Grant ANTICS 278537.
1.1 Functions with Prescribed Divisors

Let \(E\) be given over \(\mathbb{F}_q\) by an equation in the variables \(x\) and \(y\). For a rational function \(f \in \mathbb{F}_q(E) := \mathbb{F}_q(x)[y]/(E)\) and a point \(P \in E\), denote by \(\text{ord}_P(f)\) the positive multiplicity of the zero \(P\) of \(f\), the negative multiplicity of the pole \(P\) of \(f\), or 0 if \(P\) is neither a zero nor a pole of \(f\). Denote by \(\text{div}(f) = \sum_P \text{ord}_P(f)[P]\) the divisor of \(f\), an element of the free abelian group generated by the symbols \([P]\), where \(P\) is a point on \(E\).

The definition and computation of pairings involve certain rational functions with given divisors, in particular, \(f_{n,P}\) with

\[
\text{div}(f_{n,P}) = n[P] - [nP] - (n - 1)[O],
\]

the lines \(\ell_{P,Q}\) through two (not necessarily distinct) points \(P\) and \(Q\) with

\[
\text{div}(\ell_{P,Q}) = [P] + [Q] + [-(P + Q)] - 3[O]
\]

and the vertical lines \(v_P\) through a point \(P\) with

\[
\text{div}(v_P) = [P] + [-P] - 2[O].
\]

All these functions are defined up to a multiplicative constant, and they are normalised at infinity by the condition \(f(Y/X)^{\text{ord}_O(f)}(O) = 1\).

In particular, we have \(\ell_{P,-P} = v_P\), \(f_{1,P} = 1\), and \(f_{-1,P} = 1/v_P\).

The function \(f_{n,P}\) is of degree \(O(n)\) and may be evaluated in \(O(\log n)\) steps by the algorithms of \(\S3\).

1.2 Cryptographic Pairings

We quickly recall the main cryptographic pairings. In applications, they are usually restricted to \(E(\mathbb{F}_q)[r]\) in one argument and to a subgroup of order \(r\) in the other argument.

Weil Pairing

\[
e_W : E(r) \times E(r) \rightarrow \mu_r, \quad (P, Q) \mapsto (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}
\]

Computing the pairing requires the evaluation of two functions; moreover, with \(P \in E(\mathbb{F}_q)\) and \(Q \in E(\mathbb{F}_{q^k})\), the function \(f_{r,Q}\) is much costlier to evaluate by the algorithms of \(\S3\).

Tate Pairing

\[
e_T : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^r \simeq \mu_r, \quad (P, Q) \mapsto f_{r,P}(Q) \leftrightarrow f_{r,P}(Q)^{(q^k-1)/r}.
\]

The pairing requires only one evaluation of a rational function, but the original definition with a quotient group as domain is unwieldy since there is no easy way of defining unique representatives. The final exponentiation step of raising to the power \(\frac{q^k-1}{r}\) realises an isomorphism with \(\mu_r\), and the resulting pairing is usually called the reduced Tate pairing.