A Note On Compressing BN254 Curve Pairing Values

Julius Zhang

October 15, 2025

1 Introduction

This note describes the implementation of the compression method for torus-based cryptography based on [3]. We discuss various implementation details and their implications for performance. Readers interested in algorithmic details can refer to Section 2.1.

2 Compression Method

In this section, we explain the threefold compression method implemented for the BN254 curve. In the pairing computation for BN254, the second argument is an element of $E(\mathbb{F}_{q^{12}})[r]$, so the method in section 4.2 of [3] is applicable.

For notation, we consider an elliptic curve E defined over some base field $\mathbb{F}_q$ for a prime q. Common cryptographic pairings (e.g. Tate and ate pairings) take the form

$$E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] \to \mathbb{G}_r \in \mathbb{F}_{q^k} \tag{1}$$

$$(a, b) \to f(a, b)^{\frac{q^k-1}{r}} \tag{2}$$

as a bilinear map from the r-torsion points of E over some finite field extensions to the cyclotomic subgroup of order r in $\mathbb{F}_{q^k}$, where 'cyclotomic' means that the r-th power of each element in $\mathbb{G}_r$ is the identity, and $f(a, b)$ is the output of the Miller loop and the exponentiation step by $\frac{q^k-1}{r}$ is referred to as the 'final exponentiation' step in the pairing literature. In practice, one may represent the second pairing argument as the image of a point on a twist E' of the original elliptic curve E under an injective map where E' is defined over a smaller field extension for optimization.

For $k = 12$, we have

$$\frac{q^{12}-1}{r} = \Psi_6(q^2)\frac{\Phi_6(q^2)}{r}, \tag{3}$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial and $\Psi_n(x) = \frac{x^n-1}{\Phi_n(x)}$. Therefore, $f(a, b)^{\frac{q^{12}-1}{r}}$ can be computed as $f'(a, b)^{\Psi_6(q^2)}$ where

$$f'(a, b) = f(a, b)^{\frac{\Phi_6(q^2)}{r}} \in \mathbb{F}_{q^{12}}. \tag{4}$$

2.1 Threefold Compression

Let ξ be a sextic non-residue in $\mathbb{F}_{q^2}$, then $\mathbb{F}_{q^{12}} \cong \mathbb{F}_{q^2}[X]/(X^6 - \xi)$ is a sextic extension over $\mathbb{F}_{q^2}$. Moreover, let σ and τ be a quadratic and cubic root of ϵ in $\mathbb{F}_{q^2}$, respectively, we have

$$\mathbb{F}_{q^2}[X]/(X^6 - \xi) \cong \mathbb{F}_{q^2}(\sigma, \tau). \tag{5}$$

as a compositum of fields $\mathbb{F}_{q^2}(\sigma)$ and $\mathbb{F}_{q^2}(\tau)$, which are a quadratic and a cubic extension of $\mathbb{F}_{q^2}$, respectively. In particular, the q^2-Frobenius acts on $\mathbb{F}_{q^{12}}$ and interchanges σ and $-\sigma$.

We explain the threefold compression method in [3], which follows from the folllowing steps [1] to compress an element of the form $a^{\Psi_6(q^2)}$, where $a \in \mathbb{F}_{q^{12}}$. Note also that $\Psi_6(x) = (x^3 - 1)(x + 1)$.

1. Compress a^{q^6-1} to a single $\mathbb{F}_{q^6}$ element using $a^{q^6-1} = \frac{\tilde{a}+\sigma}{\tilde{a}-\sigma}$, which amounts to computing
$$\tilde{a} = \frac{a_0}{a_1} \in \mathbb{F}_{q^2}[X]/(X^3 - \xi) = \mathbb{F}_{q^2}(\tau) \cong \mathbb{F}_{q^6} \subset \mathbb{F}_{q^{12}}, \tag{6}$$
where $a = a_0 + a_1\sigma$.

2. Compute
$$\tilde{\beta} = \frac{-\tilde{a}^{q^2+1} + \xi}{-\tilde{a}^{q^2} + \tilde{a}} \in \mathbb{F}_{q^6} \tag{7}$$
where
$$\beta = \frac{\tilde{\beta} + \sigma}{\tilde{\beta} - \sigma}, \tag{8}$$
and
$$\beta = a^{\Psi_6(q^2)} = (\frac{\tilde{a} + \sigma}{\tilde{a} - \sigma})^{q^2+1} = (\frac{\tilde{a} + \sigma}{\tilde{a} - \sigma})^{q^2}(\frac{\tilde{a} + \sigma}{\tilde{a} - \sigma}) = (\frac{-\tilde{a}^{q^2} + \sigma}{-\tilde{a}^{q^2} - \sigma})(\frac{\tilde{a} + \sigma}{\tilde{a} - \sigma}), \tag{9}$$
where the last step follows from the fact that the q^2-Frobenius map is an automorphism of $\mathbb{F}_{q^{12}}$ that fixes $\mathbb{F}_{q^2}$ (and cruicially it does not fix $\mathbb{F}_{q^6}$ which is generated by τ!) and interchanges σ and $-\sigma$.

3. Express $\tilde{\beta}$ as $\tilde{\beta} = c_0 + c_1\tau + c_2\tau^2$, where $c_i \in \mathbb{F}_{q^2}$. Only store c_0 and c_1, as we can recover c_2 from c_0 and c_1 using the following equation
$$c_2 = \frac{3c_0^2 + \xi}{3c_1\xi}. \tag{10}$$

Decompression is simple: first, compute c_2 from c_0 and c_1 using (10) to recover $\tilde{\beta}$, then compute
$$a^{\Psi_6(q^2)} = \frac{\tilde{\beta} + \sigma}{\tilde{\beta} - \sigma}. \tag{11}$$

3 Implementation Details

There are various optimizations one can do to speed up the pairing calculation, which cause complication for applications that require compression, as many of these optimizations assume specific representation of the field $\mathbb{F}_{q^{12}}$ which are in conflict with assumptions in the compression method. This can cause subtle bugs that are extremely difficult to find in practice. We address several implementation details in this section.

3.1 Field Operation Optimization Specific to Field Representation

Specific optimization for field operations (e.g. [1]) routinely assume specific presentation of the field structure that can be incomptible with compression methodology. For example, the Arkworks library implements optimization in section 6.1 of [1] which assumes that $\mathbb{F}_{q^{12}}$ is built up as
$$\mathbb{F}_{q^{12}} = \mathbb{F}_{q^2}(\xi^{\frac{1}{3}})[X]/(X^2 - \xi^{\frac{1}{3}}) = \mathbb{F}_{q^2}(\xi^{\frac{1}{3}}, \xi^{\frac{1}{6}}) = \mathbb{F}_{q^2}(\xi^{\frac{1}{6}}) \tag{12}$$
which is a quadratic extension over a cubic extension of the original base field $\mathbb{F}_{q^2}$. If one uses (7) to calculate $\tilde{\beta}$ using $\tilde{a} = \frac{a_0}{a_1}$, where $\tilde{a}$ is the compressed representative of $a = a_0 + a_1\xi^{\frac{1}{6}}$, it will not work because the q^2-Frobenius map does not interchange $\xi^{\frac{1}{6}}$ and $-\xi^{\frac{1}{6}}$ which is crucial in the compression assumption.

[1] Although the paper does not mention this, the two compression steps follow conceptually from Hilbert 90 as the general statement about about the vanishing of first Galois cohomology for a cyclic extension with coefficients in the multiplicative group. When one views $\mathbb{F}_{q^{12}}$ as the tower of a quadratic and a cubic extension, Hilbert 90 states that the compression factor for norm 1 elements in the quadratic and cubic extensions are $\frac{1}{2}$ and $\frac{2}{3}$, respectively, so the total compression factor is $\frac{1}{3}$.

Fortunately, this is easy to fix via a change of basis (where recall that ξ is a sextic non-residue in $\mathbb{F}_{q^2}$ which is neither a square nor a cube):

$$\mathbb{F}_{q^2}(\xi^{\frac{1}{3}})[X]/(X^2 - \xi) \cong \mathbb{F}_{q^2}(\xi^{\frac{1}{3}})[X]/(X^2 - \xi^{\frac{1}{3}}) = \mathbb{F}_{q^{12}} \tag{13}$$

$$a + b\xi^{\frac{1}{2}} \to a + (b\xi^{\frac{1}{3}})\xi^{\frac{1}{6}}. \tag{14}$$

The map $b \to b\xi^{\frac{1}{3}}$ can be implemented using only $\mathbb{F}_{q^2}$ operations as follows

$$c_0 + c_1\xi^{\frac{1}{3}} + c_2\xi^{\frac{2}{3}} \to \xi c_2 + c_0\xi^{\frac{1}{3}} + c_1\xi^{\frac{2}{3}}. \tag{15}$$

Similarly, the inverse isomorphism is given by

$$\mathbb{F}_{q^2}(\xi^{\frac{1}{3}})[X]/(X^2 - \xi^{\frac{1}{3}}) \cong \mathbb{F}_{q^2}(\xi^{\frac{1}{3}})[X]/(X^2 - \xi) = \mathbb{F}_{q^{12}} \tag{16}$$

$$a + b\xi^{\frac{1}{6}} \to a + (b\xi^{-\frac{1}{3}})\xi^{\frac{1}{2}}, \tag{17}$$

where the map $b \to b\xi^{-\frac{1}{3}}$ can be implemented using only $\mathbb{F}_{q^2}$ as

$$c_0 + c_1\xi^{\frac{1}{3}} + c_2\xi^{\frac{2}{3}} \to c_1 + c_2\xi^{\frac{1}{3}} + (c_0\xi^{-1})\xi^{\frac{2}{3}}. \tag{18}$$

This allows one to do optimized field operations in $\mathbb{F}_{q^{12}}$ using the $\mathbb{F}_{q^6}$-basis $\{1, \xi^{\frac{1}{6}}\}$ and convert to the $\mathbb{F}_{q^2}$-basis $\{1, \xi^{\frac{1}{2}}\}$ for compression and decompression.

3.2 Final Exponentiation Optimization Specific to the Order of the Cyclotomic Subgroup

Recall the final exponentiation step computes the power

$$f^{\frac{q^{12}-1}{r}} = f^{\Psi_6(q^2)\frac{\Phi_6(q^2)}{r}}. \tag{19}$$

This is usually done by raising to the exponent $\Psi_6(q^2)$ first, which enables further opportunities applicable as $f^{\Psi_6(q^2)}$ has order $\Phi_6(q^2)$, where faster inverse and squaring methods in a cyclotomic subgroup of that order are possible [2]. However, since we compress the $\Psi_6(q^2)$ power of a field element, it appears one needs to do the $\Psi_6(q^2)$ power last which makes it hard to apply the cyclotomic inversion and squaring techniques, as the input may not have order $\Phi_6(q^2)$.

3.3 Operations Done on Compressed Values

In [3], the authors describe various techniques for computing the line functions as part of the Miller loop on compressed field elements. We do not implement these for applications that are not memory bound.

4 Performance Evaluation

The compression only affects the final exponentiation step of the pairing computation and therefore the overhead decreases as the number of pairs in the multi-pairing computation increases. See Table 1 for performance comparison with uncompressed multi-pairing.

Table 1: Compressed Multi-Pairing Computation Time (microseconds)

	1 Pair	5 Pairs	100 Pairs
Compressed	0.938	1.617	17.913
Uncompressed	0.514	1.172	17.068

References

[1] Augusto Jun Devegili, Colm Ó hÉigeartaigh, Michael Scott, and Ricardo Dahab. Multiplication and squaring on pairing-friendly fields. Cryptology ePrint Archive, Paper 2006/471, 2006.

[2] Walid Haddaji, Loubna Ghammam, Nadia El Mrabet, and Leila Ben Abdelghani. Efficient pairings final exponentiation using cyclotomic cubing for odd embedding degrees curves. Cryptology ePrint Archive, Paper 2025/958, 2025.

[3] Michael Naehrig, Paulo S. L. M. Barreto, and Peter Schwabe. On compressible pairings and their computation. Cryptology ePrint Archive, Paper 2007/429, 2007.