# Bandersnatch

by Simon Masson (Anoma - https://anoma.network/) and Antonio Sanso (Ethereum Foundation - https://ethereum.foundation/)

This document describes the details of Bandersnatch

a new elliptic curve built over the BLS12-381 scalar field. The curve is similar to Jubjub but is equipped with the GLV endomorphism hence it has faster scalar multiplication.

[

drawing

800×1237 327 KB

](https://ethresear.ch/uploads/default/original/2X/5/5dba0aa21255f9e29febf734582f19b3d2b8b8ce.jpeg)

## BlS12-381 and Jubjub

BLS12-381 is a pairing friendly curve created by Sean Bowe in 2017. Currently BLS12-381 is universally recognized as THE PAIRING CURVE

to be used given our present knowledge

(cit.).

The ZCash team also introduced a new curve built over the BLS12-381 scalar field: Jubjub.

JubJub is a twisted Edwards curve that can be made efficient inside of the zk-SNARK circuit.

## Introducing Bandersnatch

In order for some cryptographic application to scale it is needed to have a curve like Jubjub but with faster scalar multiplication. One efficient way to speed scalar multiplication up is to employ the celebrated GLV endomorphism (also used by the “Bitcoin curve”

- secp256k1). This technique was until few months ago protected by a US Patent that is now expired and freely usable.

We performed an exhaustive search of curves where the GLV endomorphism could be used over the BLS12-381 scalar field using the Complex Multiplication (CM) method of generating an elliptic curve. To be more specific we computed the order of such curves for the discriminants from -1

to -388

.

We found one suitable curve for discriminant -8

with order 2^2\cdot 13108968793781547619861935127046491459309155893440570251786403306729687672801

Bandersnatch is also twist secure: the order of the twist is 2^7 \cdot 3^3 \cdot 15172417585395309745210573063711216967055694857434315578142854216712503379

The curve has j-invariant equal 8000

and exhibits 125.75

bit security . Given the shape of the order it can be expressed also in Montgomery and Edward form.

Bandersnatch in twisted Edwards form looks like

$-5x^2+y^2 = 1+dx^2y^2$

with d=\frac{138827208126141220649022263972958607803}{171449701953573178309673572579671231137}

.

### Bandersnatch’s endomorphism

The endomorphism of degree 2 is defined by

$\psi(x,y,z) = (xa_1(y+a_2z)(y+a_3z), b_1(y+b_2z)(y+b_3z)yz^2, (y+c_1z)(y+c_2z)yz^2)$

and can be computed in 17 multiplications and 6 additions modulo $p$

$(a_i, b_i, c_i$

are integers modulo $p$

).

## Scalar multiplication improvement

From the efficient endomorphism $\psi$

, it is easy to apply the GLV method and improve the scalar multiplication cost:

- Roughly, a scalar multiplication $[n]P$

cost $(\log n) \text{Dbl} + (\log n/2) \text{Add}$

.

- Using the GLV endomorphism, we can compute $[n]P$

using $(\log n/2 )\text{Dbl} + (3\log n/8) \text{Add}$

, plus few precomputations.

We performed python

benchmarks between the double-and-add algorithm and the GLV method applied in the case of our curve, and the GLV version is 30% faster

.

Acknowledgments:

we would like to thank Luca De Feo, Justin Drake, Dankrad Feist, Daira Hopwood and Zhenfei Zhang for fruitful discussions.