Hello,

My name is Dimitri Koshelev. I am a researcher from Moscow and Paris. My field of science is pairing-based cryptography.

I invented a new very efficient point compression-decompression method for any elliptic curve E

of j-invariant 0 over finite fields. It is well known that these curves are widely used in pairing-based cryptography, in particular in Ethereum. If I am right this is an actual task.

Let \mathbb{F}_q

be a finite field and \mathbb{F}_{q^2}

be its quadratic extension. My method can be implemented in two different ways, namely for the simultaneous compression (to 2\log_2(q) + 3

bits) of two \mathbb{F}_q

-points (or one \mathbb{F}_{q^2}

-point) of E

. The new method is much more efficient than classical one with x-coordinates, because at the decompression stage it requires to accomplish only 1 exponentiation in \mathbb{F}_q

instead of 2.

Please, see the preprint of my article if you want. In the work I use quite complicated mathematics, but eventually produce explicite quite simple formulas of compression and decompression.

Maybe one of Ethereum developers will decide to use my formulas for an optimization of the cryptocurrency. If you are interested, then I can help, sending the formulas written in one of programming or computer algebra languages.

Sincerely yours, Dimitri.