Hello,

Earlier I posted the topic [A new point compression-decompression method for any elliptic curve of j-invariant 0] about my new article. It proposes a new compression method for points from $E(\mathbb{F}_{!q^2})$, where $E!: y^2 = x^3 + b$ is an elliptic $\mathbb{F}_{!q^2}$-curve of j-invariant 0. Unfortunately, that article is very difficult to understand, because it contains non-trivial facts from algebraic geometry.

Thus I decided to write a new very simple article consisting of 4 pages and clarifying my ideas without any facts from algebraic geometry. The abstract of this article is the following.

The article provides a new double point compression method (to $2\log_2(q) + 4$ bits) for an elliptic $\mathbb{F}_{!q}$-curve $E!: y^2 = x^3 + b$ of j-invariant 0 over a finite field $\mathbb{F}_{!q}$ such that $q \equiv 1 \ (\mathrm{mod} \ 3)$. More precisely, we transform the coordinates x_0,y_0,x_1,y_1 of two points $P_0, P_1 \in E(\mathbb{F}_{!q})$ to the elements $x_0/x_1, y_0/y_1$ with four auxiliary bits. To recover (in the decompression stage) the points P_0, P_1 it is proposed to extract a sixth root $\sqrt[6]{w} \in \mathbb{F}_{!q}$ of some element $w \in \mathbb{F}_{!q}$. It is easily seen that for $q \equiv 3 \ (\mathrm{mod} \ 4)$, $q \not\equiv 1 \ (\mathrm{mod} \ 27)$ this can be implemented by means of just one exponentiation in $\mathbb{F}_{!q}$. Therefore the new compression method seems to be much faster than the classical one with the coordinates x_0, x_1, whose decompression stage requires two exponentiations in $\mathbb{F}_{!q}$.

Please, see [the preprint of the new article] and let me know if you are interested. Maybe one of Ethereum developers will decide to use my formulas for an optimization of the cryptocurrency.

Sincerely yours, Dimitri.