Let me create the topic in which we will discuss how to rapidly generate "independent'' points on elliptic curves. I wrote an article, where this cryptographic primitive is considered in detail. There I explain why it is important. Besides, I invent a new generation method based on some lattices. If you wish, read at least the following abstract of my article.

The article develops a novel method of generating ``independent'' points on an ordinary elliptic curve E

over a finite field. Such points are actively used in the Pedersen vector commitment scheme and its modifications. In particular, the new approach is relevant for Pasta curves (of j

-invariant 0

), which are very popular in the given type of elliptic cryptography. These curves are defined over highly 2

-adic fields, hence successive generation of points via a hash function to E

is an expensive solution. Our method also satisfies the NUMS (Nothing Up My Sleeve) principle, but it works faster on average. More precisely, instead of finding each point separately in constant time, we suggest to sample several points at once with some probability.

In the future I hope to continue research in this direction in order to produce an even faster generation method.