Matrix Multiplication parameters calculations (?)

P - a bunch of HElib's parameters (include p, r, m and others)

n(P) - the **nslots** value for the parameters params

M(x) - a square matrix of size x*x

Enc(params) - the time (in clock ticks or milliseconds) takes to encrypt M(n(P)) **on user's machine**

Dec(params) - the time (in clock ticks or milliseconds) takes to decrypt M(n(P)) **on user's machine**

NaiveMul(x) - the time (in clock ticks or milliseconds) takes to multiply 2 M(x) in naive way (PT matrices, without any HE)

for multiply 2 square matrices of size N (M(N)), we want to find P (parameters) such:

$$(\frac{N}{n(P)})^2(2*Enc(P)+Dec(P)) < NaiveMul(N) = (\frac{N}{n(P)})^3 NaiveMul(n(P))$$

$$2*Enc(P)+Dec(P) < (\frac{N}{n(P)})NaiveMul(n(P))$$

when $(\frac{N}{n(P)})^2$ is the number of M(n(P)) in M(N). So:

$$N > \frac{n(P)*(2*Enc(P)+Dec(P))}{NaiveMul(n(P))}$$

Note: these calculations not include the time it takes to send the data to the server, and the time it takes to receive it.

Send(x) - the time it takes to send data with total size of x to the server

Rec(x) - the time it takes to receive data with total size of x from the server

$$N > \frac{n(P)*(2*Enc(P)+Dec(P)+2*Send(M(n(p)))+\mathrm{Re}c(M(n(p))))}{NaiveMul(n(P))}$$

This inequality add the time it takes to send each M(n(p)) (2 times because 1 of each matrix) and the time it takes to receive it back from the server.

Another thing that is missing here is the time it takes to the server to calculate the multiplication itself. In the previous calculations, we assumed it 0 for super powerful cloud server.

let FHE_Mul(x) be the time it takes to the server to multiply 2 encrypted M(x), so:

$$(\frac{N}{n(P)})^2(2*Enc(P)+Dec(P)+2Send(M(n(p)))+\mathrm{Re}c(M(n(p))))+(\frac{N}{n(P)})^3 FHE\_Mul(n(p)) < (\frac{N}{n(P)})^3 NaiveMul(n(P))$$

$$(2*Enc(P)+Dec(P)+2Send(M(n(p)))+\mathrm{Re}c(M(n(p))))+(\frac{N}{n(P)})FHE\_Mul(n(p)) < (\frac{N}{n(P)})NaiveMul(n(P))$$

$$(2*Enc(P)+Dec(P)+2Send(M(n(p)))+\mathrm{Re}c(M(n(p)))) < (\frac{N}{n(P)})(NaiveMul(n(P))-FHE\_Mul(n(p)))$$

$$N > \frac{n(P)(2*Enc(P)+Dec(P)+2Send(M(n(p)))+\mathrm{Re}c(M(n(p))))}{NaiveMul(n(P))-FHE\_Mul(n(p))}$$