The Challenge of the Petaflops

The news.

Last year the news came out that the United States of America had recovered first place in the supercomputer environment with the supercomputer Summit, with a performance of 200 petaflops/sec.

On the 21st of September the news commenting the announcement by sources close to Google was published by Charles Plateau of Reuters which assured that Google had succeeded in the development of a quantum supercomputer that in 3 minutes and 20 seconds did the calculations corresponding to an algorithm that in the Summit supercomputer requires 10,000 years of continuous work.

However, it is commented that it only applies to specific technical problems and that we are still several years away from solving various computational problems. But assuming in good faith that at the rhythm of the advance of computational hardware, this delay can be solved in five years, it can be stated that we are on the brink of a scenario that places on the spot the key dependent symmetrical cryptographic classic algorithms like AES 256.

In this regard, if we homologate the speed of the said quantum machine to petaflops/sec, the following turns out:

The quantum speed:

How many seconds are there in 10,000 years?

In one day there are 86,400 seconds and in one year = 31,536.00 that is $\mathbf{3.1536 \times 10^7}$ seconds.

Given that Summit performs 200 petaflops every second (floating point operations).

One petaflop is equal to 10^{15} floating point operations. Therefore 200 petaflops are equivalent to 2×10^{17} floating points operations.

Then in 10,000 = (10^4) years the Summit computer can perform:

$(2 \times 10^{17}) \times (3.1536 \times 10^{11}) \times (10^4) = 6.307 \times 10^{32}$ floating point operations per second (flops).

If we divide the previous figure by the time it took the aforementioned quantum computer (3 minutes and 20 seconds = 200 seconds), it turns out that the yield of that computer is:

$$(6.307 \text{ x } 10^{32}) / (2 \text{ x } 10^{2}) = 3.1535 \text{ x } 10^{30} \text{ flops.}$$

This figure can be compared with the Gedaken (idealized experiment) proposed in the document “Cyphertop’s Resistance to Computational Brute Force Attacks”. And from such comparison, the conclusions that follow are extracted.

The current cryptographic risk:

In the mentioned document the existence of a quadrillion “improved” Summit computers is assumed, that is, each one of them is a quadrillion times more powerful that the current Summit. The computational force of such a grid of “improved” Summit supercomputers would be 2 x 10^{41} flops. And as it was mentioned in that document, not even with that computational force operating till the end of our physical universe, the Cyphertop code can be broken, much less with the power of the recently announced quantum supercomputer: 3.1535 x 10^{30} flops.

Now, with regard to the AES 256 algorithm, we have that the complexity or strength of it is equal to 255^{32}. This is equivalent to 1,02161150204 x 10^{77}.

Although for now, it remains safe, it is to be expected that another “giant” leap, like the one just announced in the development of quantum hardware, can jeopardize it at any moment since its security margin has been reduced more than one third in what is expected traditionally.

Cyphertop with its strength estimated at **1.7135447658999 x $10^{60,318}$**, has nothing to worry about, not even remotely.

ADVM SECURITY SOFTWARE C.A.