Proposing a Quantum simulator for integer factorization[1]

Jose Luis Rosales, Vicente Martin†

Center for Computational Simulation, Universidad Politécnica de Madrid, Boadilla del Monte, Madrid 28660, Spain.

† e-mail:vicente@fi.upm.es; e-mail:jose.rosales@fi.upm.es

ABSTRACT.—

Many cryptographic algorithms depend on computational complexity assumptions. Notorious cases are the RSA algorithm for public key criptography or the Diffie-Hellman key exchange protocol, to publicly agree on a common secret key. Both algorithms are known to be broken by quantum computing as well as those that can be reduced to a discrete logarithm problem. These are key algorithms in our digital society and are at the basis of everyday tasks, specially those that rely on digital signatures. The RSA algorithm, in particular, is probably the most used algorithm and is its assumed security the one that guards most of the e-commerce nowadays. In this case, it is the time complexity of finding the prime factors of a large number, that grows worse than polinomially with the size of the number, the manin guardian of our cyberinfrastructure. The fact that a quantum computer can solve this problem in polynomial time using Shor's algorithm is seen as a potentially major disruption and has prompted security agencies to advice the progressive deprecation of these algorithms[2].

However, the practical realization of quantum computers able to implement the Shor's algorithm to factor numbers of the size used in the day to day use of RSA, is still years in the future. The typical implementations of Shor's algorithms use the gate model of quantum computing, but another possibility would be to build the solutions in Hilbert space of a quantum simulator performing factorization, instead of going through the route of a gate-based, fully programmable, quantum computer. The key idea, following the pioneering suggestions of Feynman[4], is to translate factoring arithmetics into the physics of a device whose superposition of states mimics the problem i.e.: a factoring (analog) computer. The states of the simulator would be the solutions of some hermitian operator depending only on the number that we want to factorize. This is an "analogue" computer in the sense that it is not like the Shor's

[1]Parts of this contribution are under revision in Phys. Rev. Lett.

algorithm, programmed in a quantum computer following the gate model; it is the measurement of a carefully set quantum system what provides the answer.

To carry out this program, an arithmetic formulation of the factorization problem that is amenable to be quantized is devised. An arithmetic function, eventually related to a Hamiltonian, and the quantum-mechanical problem such that its solution corresponds to the solution of the factorization problem is set up. To have a discrete spectrum, the Hamiltonian must also be bounded. Also, to go beyond the formulation of the problem in quantum terms and actually solve it, an adequate arithmetic function and boundary conditions must be found. In this contribution, we present a correct arithmetic function, defined the factorization set to bind the Hamiltonian and obtained the solution of the quantum-mechanical problem. We show that the quantum theory of factoring a number N into its co-prime factors requires to build a Feynman simulator whose spectrum of eigenvalues corresponds to a quantum anharmonic oscillator. To the best of our knowledge, this has not been achieved before, although ours was not the first attempt.

To validate the results obtained, we have proved its predictive capabilities: obtained a factorization algorithm that is completely new, with no similitude to any other factorization algorithm that we know of, and thoroughly checked the statistics of the solution against the prime number theorem. We show how the algorithm, that is obviously different from any kind of classical sieve, is able to factor numbers better than a random search –that can be considered as the null hypothesis– thus showing that there is additional "quantum information" introduced by the algorithm. Note, however, that the algorithm is essentially a numerical simulation of a quantum-mechanical device. Its aim is, apart from demonstrating the possibility of conceiving a classical factoring algorithm from very different principles than the traditional ones, to show that the quantum simulator will perform as expected. Finally, although not less important, we also show that the statistics from the simulator is correct: the spectrum reproduces the prime counting function and is almost identical to the Riemann's function, the best approximation known. This is obtained as a direct consequence of the quantum mechanical theory and has no counterpart in number theory. Carrying this to the extreme, this could be even considered the physics underlying the Riemann's hypothesis in the sense that the Hamiltonian is naturally bounded, without any further assumptions.

1. What follows is an outline of the contents that would be included in the poster.

Statement of the problem and definitions.— Suppose that we have to find the divisors for the following numbers, say $N_1 = 10^{19} + 192309 = 1590452701 \cdot 6287518009$ and $N_2 = 10^{19} + 112533 = 2646394187 \cdot 3778726559$, we expect to require the same number of trial divisions, since $\pi(\sqrt{N_1}) = \pi(\sqrt{N_2})$ is the maximum number of prime factor candidates

in both cases[2]. There are many of these numbers being product of two primes with the same property; we'll say that N_1 and N_2 belong to the same **factorization ensemble** $\mathcal{F} = \{N_k : \pi(\sqrt{N_k}) = j\}$.

According to the prime number theorem, these numbers can be parameterized as $N_k = x_k y_k \sim (\sqrt{N} + \sigma_k \ln\sqrt{N})^2$ and $\sigma_k = O(1)$. Thus, in our example, we can safely take $N = 10^{19}$. This is a bounded set. If N is the number to factorize, the asymptotic value of possible pairs of coprimes candidates in $\mathcal{F}$ is a huge number: $|\mathcal{F}| \sim \sqrt{N} \ln\ln\sqrt{N}$.

A different way to look at the problem of factoring $N = xy$ is, therefore, to obtain single-valued arithmetic functions defined in $\mathcal{F}$ depending only on x and y. For instance, the arithmetic functions

$$E = \pi(x)\pi(y)/j^2,\ p = (\pi(y) - \pi(x))/2j,\ q = (\pi(y) + \pi(x))/2j \tag{1}$$

are unique in $\mathcal{F}$ acording to Euclid's factorization theorem. This is relevant since, given that E is a new - unknown- constant, we can re-formulate the problem of factoring N into that of finding E in $\mathcal{F}$ for a given N in that ensemble.

Quantum simulator.— The three arithmetic functions in 1 are related, i.e., E is the only unknown constant of the problem

$$p^2 + V(q) = -E/2, \tag{2}$$

for $V(q) = E/2 - q^2$. This represents a classical anharmonic oscillator. Remarkably, the coordinate q and the momentum p are bounded in $\mathcal{F}$ and so is E, meaning that the operator

$$H = P^2 + V(Q), \tag{3}$$

is Hermitian in the corresponding quantum theory; the eigenfunctions satisfy the Schödinger equation

$$[-\nabla^2 + V(Q)] \cdot \psi(Q) = -\frac{E}{2}\psi(Q). \tag{4}$$

We can consider this as the conditions of a Feynman analog computer of factoring that obtains as eigenvalues the arithmetic function E, provided that the appropriate limits in $\mathcal{F}$ are imposed for the coordinate $Q = Q_o(N)$. The equation corresponds to a trapped particle in a box that tunnels to the right (symetrically to the left) of a potential barrier $V(Q)$:

$$\Psi(Q) = \psi(Q)\psi(-Q).$$

Remarkably the trapped particle should have a symetric wave function and, therefore, it should be a boson. The solution for the stationary state is represented in Fig.1.

A quantum enhanced algorithm.— Selecting for the size of the box $Q_o(N) = O(N^{1/6})$, the number of possible outputs, $T(N)$, of the simulator scales logarithmicaly in N, i.e.: it is polynomial in the number of bits of N.

$$T(N) = (32\pi/3)(\ln\sqrt{N})^3.$$

[2] $\pi(x)$ is the prime number counting function, that counts the number of primes less or equal than x.

This is consistent with Shor's [1] estimates for the quantum solution complexity of the problem.

From the spectrum of the simulator, the primes can be obtained. The steps of the algorithm are:

- Obtain E_k solving Eq. 4 in the factorization ensemble $\mathcal{F}(j)$
- Since $k \leq |\mathcal{F}(j)|$ and the statistics of the primes in $\mathcal{F}(j)$ is known, there exist $x(k)$.
- Find $E(k(x))$.
- Obtain $\pi(x) = \frac{j^2}{\pi(N/x)} E(k(x))$

This $\pi(x)$ is plotted in Fig. 2.

Moreover, the spectrum allows for a new algorithm of factorization. The $x_k = f(E_k)$ are the quantum predictions for the factor. However, as it was pointed out by Feynman [4], one can not simulate quantum physics with a classical computer. This means that singling out, classically, a preferred value of the state k to start our search is not possible. All that can be done is to compute the whole E_k set and paralellize our search - since every state is independent from each other. To test the algorithm we can compare a classical algorithm doing a search using $(\ln \sqrt{N})^3$ random starting points –what we call here, null hypothesis– versus the same search starting in the quantum predictions. To show this we have changed the variables to the relative distance of the correct factor, x, to the best predicted point (i.e. the point that has the factor x in its close vecinity):

$$\xi = |x - x_k|/x$$

The expected distribution of the random solutions is a gaussian of width $\sigma \sim T(N)/(j\sqrt{(N)})$ whereas a much narrower one is expected if the quantum algorithm is better at predicting the factors. This would be a result of the new quantum information brought about by the quantum solution. This is depicted in Fig. 3.

RESULTS.— Fig. 1, Fig. 2 and Fig. 3 summarize the results.

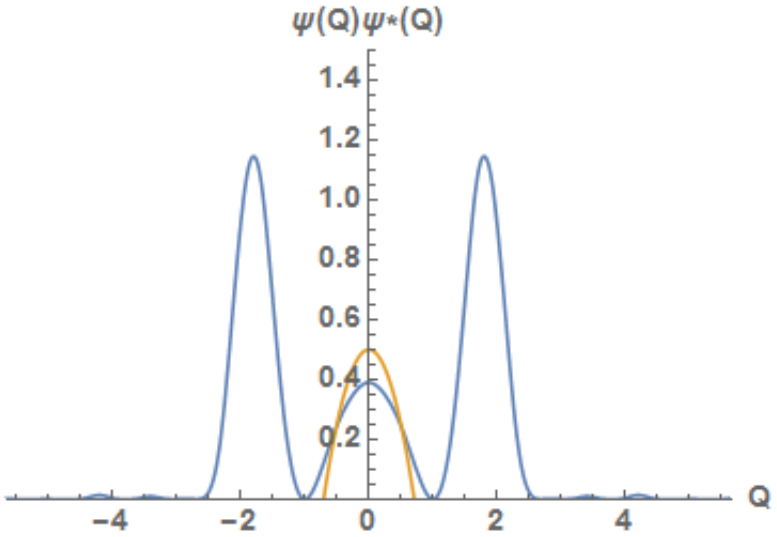

Fig. 1. Trapped boson through the potential barrier probability distribution for the quantum stationary state (in blue). It represents the solution of a quantum simulator of factoring. The limits of the coordinate depend only on N while the height of the barrier (in orange) and the peaks of maximum probability signal a factor of N.

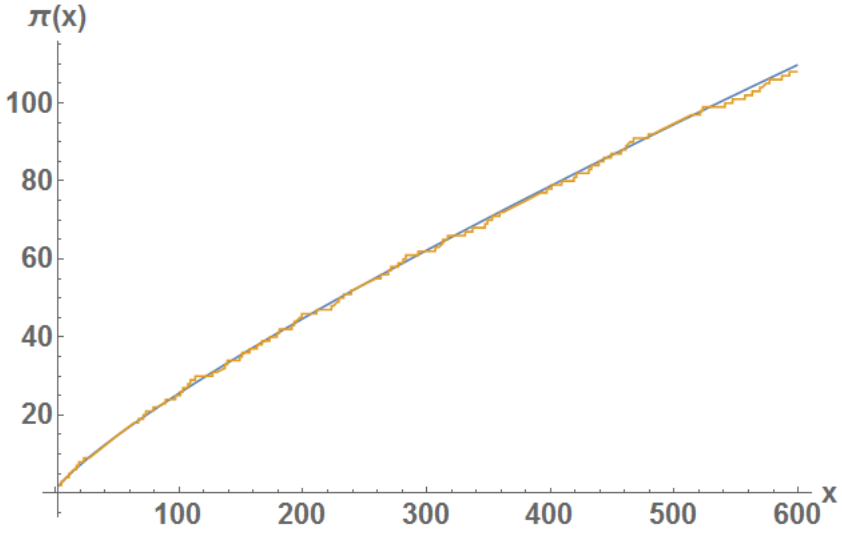

Fig. 2. Approximation to $\pi(x)$ obtained by the simulator. Note its extreme precision, meaning that the solutions of the simulator reproduce the statistics of the primes

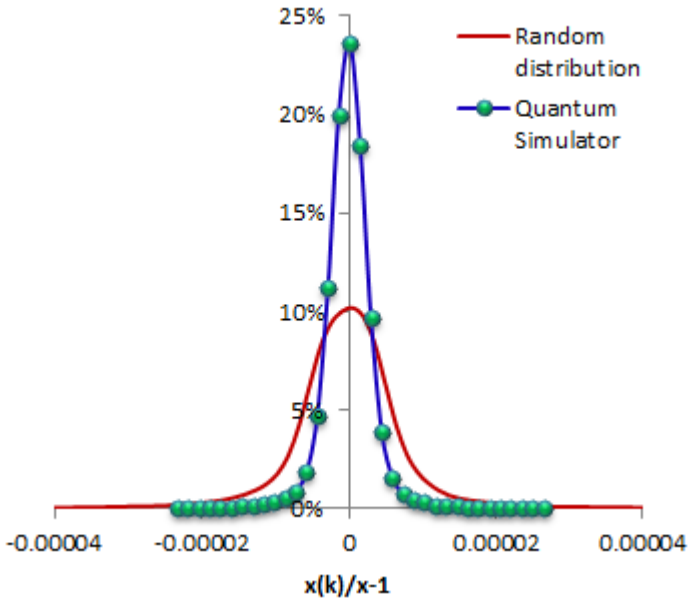

Fig. 3. Histogram of the statistical variable $\xi = (x(k) - x)/x$ for 33000 factorizations. We applied the quantum spectrum of the simulator to find factor candidates for $N = 10^{22} + a$, $a < 10^{11}$ being

product of two primes. It represents the frequency of achievable relative distance for the closest eigenvalue to the actual factor. For the sake of comparation –calculated for the same number of random distributed points–, simple Montecarlo searches that assume a uniform distribution of the primes (null hypothesis) are also depicted (red Gaussian). The difference in the width of the two peaks is a signature of the new quantum information that the simulator brings to the problem. A random search produces a width of the order of $T(N)/(j\sqrt{(}N))$, whereas the quantum search gives a much smaller one.

CONCLUSIONS. We propose a quantum simulator of factoring. This can be tested both theoretically (optaing the distribution of the primes from quantum theoretical considerations) and in a future experimental set up as suggested here. Moreover we directly derived a quantum enhanced algorithm of integer factorization that uses additional information that comes from quantum theory.

ACKNOWLEDGMENTS.— Supported by Quantum Information Technologies Madrid+ (QUITEMAD+), S2013/ICE-2801, funded by *Comunidad Autónoma de Madrid*.

References

[1] Shor, P.W. "Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.

[2] `https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml`, Reviewed: Aug 19, 2015

[3] Rosales, J.L and Martin, Vicente "On the Quantum Simulation of the Factorization Problem", http://arxiv.org/abs/1601.04896.

[4] Feymann R., Inter. J. Mod. Phys. 21,6/7, 1982 pp 467 − 488.