Quantum Abracadabra

Karl Svozil

Institute for Theoretical Physics, Vienna University of Technology,

Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria and

Department of Computer Science, University of Auckland,

Private Bag 92019, Auckland 1142, New Zealand[*]

[*] svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

In private conversations, the late Swiss mathematician Ernst Specker related "Jesuit lies" to distorting facts without lying explicitly – by either issuing ambiguous statements, or by stating only the convenient facts while omitting inopportune ones, or by allowing outrageous claims without correcting them – if only it is advantageous. It should come as no surprise that these sort of issues also occur in science; in particular, if resources and big money are involved. What makes this worrisome is the fact that, unlike politicians and just as theologians, scientists have great authority regarding the pursuit of truth. As a consequence, the public, and political bodies and institutions, tend to uncritically adapt exaggerated, biased claims as matters of fact; in particular, if it serves some profits and the public's desire for fairy tales.

A striking example are the nuclear power plants in Three Mile Island, Chernobyl, and Fukushima falsifying bold claims that nuclear fission technology is "safe beyond doubt."

In a similar fashion, the alleged mysteries of the quantum has been sold to the public for quite some time now. The "quantum mechanics is magic" tour, expressed for instance in Europe's quantum community's *Quantum Manifesto,* has, among other, previous initiatives world-wide, recently launched a European €1 billion quantum technologies flagship initiative in quantum technology. The campaign promises to initiate nothing less than a second quantum revolution.

I have no doubts that €1 billion spent on the quantum are wisely invested, and that something worthy will come out of it. Alas what leaves me worried is the deceptive and potentially harmful way this, and similar, quantum related initiatives are marketed. While many of the Quantum Manifesto's short- and medium-term goals appear feasible, some of the long-term goals might not even be achievable in principle. And when it comes to quantum random number generators and quantum cryptography, certain goals are provable impossible.

Let us, for the moment, contemplate on the Manifesto's call to *"build a universal quantum computer able to demonstrate the resolution of a problem that, with current techniques on a supercomputer, would take longer than the age of the universe."* I am at a loss of imagining what that could be; given the rather sober situation regarding the capacity of quantum computers. Although NIST's *Quantum Algorithmic Zoo* enumerates a growing number of potential speedups, no substantial "killer-apps" have been suggested in the last years, and there does not even exist a consolidated view about what exactly could

make quantum computation superior over classical computation. Most observers seem to agree that one advantage might be quantum parallelism: based on coherently superposing classically distinct and mutually exclusive computational states, the capacity to push all of them through a quantum computer simultaneously. Alas, there's a "Hamletian rub:" the operator has no direct access to the state processed, and has to analyse the output state subject to complementarity. It seems that this strategy is applicable only in particular instances, in which certain properties can be encoded into suitable orthogonal subspaces. In such cases, relational information about the input-output behaviour can be extracted from such states without the need (or possibility) to analyse the single cases contributing to the correlations.

It also remains unclear whether quantum computation is scalable in the sense that an increase in quantum bits needs no excessive, possibly exponential, overhead in resources creating and maintaining the additional bits.

Another quantum asset is the use of entanglement for communication involving multiple particles across arbitrary distances. Such a system could be in a definite collective state, defined solely in terms of relational properties or correlations among the constituents, whereas the states of the single constituents remain totally undefined. While in this regard exponential speedups have been proposed, there is again no common understanding of the issues involved.

With regards to quantum random number generators, the situation is confused, to say the least. Indeed, it is not even clear where exactly quantum randomness resides: it cannot originate from elements such as lossless beam splitters, because these are merely permuting the quantum state. If measurements were the source of randomness, then it would be means relative at best.

Moreover, because of incompleteness theorems such as the recursive unsolvability of the halting and the rule inference (induction) problem, any statement regarding the *ex nihilo* creation of empirical bit sequences are provable unprovable. Thus regardless of what we may be inclined to believe, and whatever authoritative certificates are issued, such claims remain strictly metaphysical and conjectural.

Finally, contrary to publicized claims, quantum cryptography is insecure and can be successfully cryptanalyzed through man-in-the-middle attacks. Already Bennett and Brassard acknowledged this possibility by discussing active eavesdropping. As a

consequence, such quantum cryptographic protocols, in order to be safe, require both an uncompromised classical as well as quantum communication channel. With these provisos one may ask, what exactly is the advantage and the "added security?" Is quantum cryptography presenting itself as the solution of a problem while at the same time requiring the absence of this threat it purports to resolve? If you push the experts with these kind of questions, they respond that, rather than generating a key out of the blue, within certain error bounds, they could "enlarge" an existing key. This is the type of confidence that is implied by "unconditional security" in many of these papers.

Let me finish by suggesting that, besides all the aforementioned quantum challenges, we desperately need an entirely different initiative; this one requiring much higher "whatever it takes" investments: thermonuclear fusion might be sustainable at moderate operating costs and perils. The sooner we seriously start investigating this potential energy resource, the smoother physics might be able to provide solutions to the upcoming energy crisis, with depleting cheap crude oil.

ACKNOWLEDGMENTS

This work was supported in part by the European Union, Research Executive Agency (REA), Marie Curie FP7-PEOPLE-2010-IRSES-269151-RANPHYS grant.

Responsibility for the information and views expressed in this article lies entirely with the author. The content therein does not reflect the official opinion of the Vienna University of Technology or the University of Auckland.

The author declares no conflict of interest and, in particular, no involvement in nuclear fusion research.