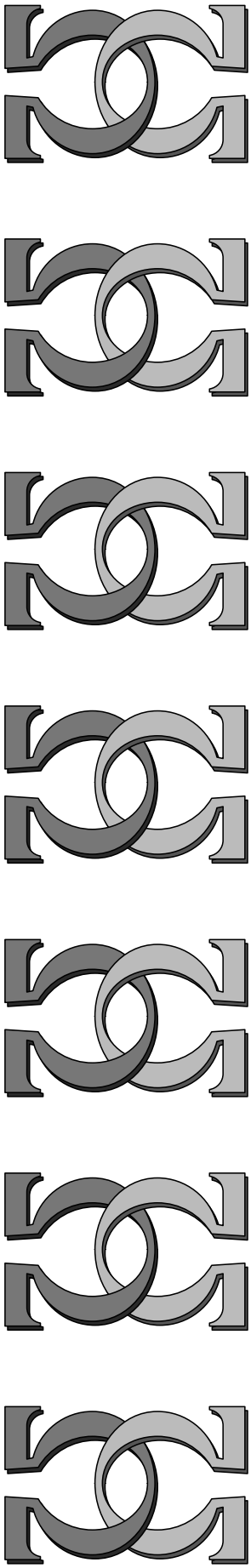

CDMTCS
Research
Report
Series

Quantum Informatics and the Relations Between Informatics, Physics and Mathematics: A Dialogue

C. S. Calude, J. Gruska
University of Auckland, NZ
Masaryk University, Czech Republik

CDMTCS-306
April 2007

Centre for Discrete Mathematics and
Theoretical Computer Science

Quantum Informatics and the Relations Between Informatics, Physics and Mathematics: A Dialogue

C. S. Calude, *University of Auckland, New Zealand*
J. Gruska, *Masaryk University, Czech Republik*

Professor Gruska (`http://www.fi.muni.cz/usr/gruska`) *is well known not only for his results but also because he was "everywhere"—he had 33 long term visiting positions in Europe, North America, Asia, and Africa. He is a pioneer in descriptional complexity (of grammars, automata and languages). Professor Gruska is cofounder of four regular series of conferences in informatics and founding chair (1989–96) of the IFIP Specialist Group on Foundation of Computer Science that resulted in the establishment of the IFIP Technical Committee TC1, Foundations of Computer Science. Professor Gruska other research interests include parallel systems and automata, and, more recently, quantum information processing, the subject of this dialogue—C.S.C.*

Cristian Calude: A century ago hardly anyone would consider information an important concept for physics.

Jozef Gruska: Correct. One can even say that at that time one could hardly see information as a scientific concept at all. In spite of the fact that quantum entropy had been known since 1932, and actually before the classical entropy, it was only due to the seminal work of Shannon, *A mathematical theory of communication*, in 1948, that (hard) science started to see the concept of information as a scientific one.

CC: Shannon's concept is very important, but it does not fully capture the intuitive concept of information. There are many other models for information (a "Workshop on Information Theories" was held in Münchenwiler, Switzerland, in May 2006).

JG: I think philosophers still consider the concept of information as one we have no full understanding yet. Historically, they see its origin from the Latin words *informatio* and *informare*. In Scholastic one would see information as *representation of matter through a form*. Information usually has three dimensions: syntax, semantics, and pragmatic. An important philosophical approach to this concept was developed by Carl Friedrich Weinzsäcker with his *Information is das Maß eine Menge von Form ...*; it comes from his *Ur-Theorie*. Sadly, Weinzsäcker died on April 28, 2007, at the age of almost 95. There are lots of interesting materials written about *information* from the point of view of philosophers, but hardly something "really useful". Shannon's approach, motivated to a significant extend by war problems, considers "only" quantitative aspects of information, from the point of view of transmission, as a key ingredient of communication. This semantics-less concept has turned out to be extremely important and a success story of modern (applied) mathematics.

CC: My colleague, Garry Tee, pointed out to me that Edmond Halley published his great geomagnetic map of the Atlantic Ocean already in 1699, and for centuries thereafter immense efforts were devoted to measuring precise information about the Earth's magnetic field. And from 1850 to 1890 Kelvin, Maxwell, Jenkin, Rayleigh and other British physicists devoted immense efforts to establishing accurate measurements in electricity. However, probably the first important use of information in a more abstract way in physics was related to an explanation of the Maxwell demon paradox.

JG: A significant breakthrough in the views on the relation between physics and information came, I think, actually only after Landauer's observation that *information is physical*: physical carriers are needed to store, transform and transmit information and therefore the laws and limitations of physics determine also the laws and limitations of information processing. An additional breakthrough came later with the view usually attributed to John Wheeler: *physics is informational*. Information processing phenomena, as well as their laws and limitations, are of key importance for understanding the laws and limitations of physics.

CC: Wheeler summarised his position with the now famous "It from bit" (*Sakharov Memorial Lectures on Physics*, vol. 2, Nova Science, 1992). This "thesis" is well discussed in many publications, for example in Tom Siegfried's book *The Bit and the Pendulum* and in Seth Lloyd's book *Programming the Universe*.

JG: Wheeler explained in more details his position as follows: "*It from bit* symbolises the idea that every item of the physical world has at the bottom—at the very bottom, in most instances—an immaterial source and explanation. Namely, that which we call *reality* arises from posing of yes-no questions, and registering of equipment-invoked responses. In short, that things physical are information theoretic in origin."

Of interest is the following Wheeler's confession: "I think of my lifetime in physics as divided into three periods: In the first period ... I was convinced that everything is particles; I call my second period everything is fields; now I have a new vision, namely that everything is information".

CC: Wheeler's position is close to digital physics (a term coined by Fredkin), which proposes to ground much of physical theory in cellular automata by assuming that the universe is a gigantic universal cellular automaton. Gregory Chaitin, Edward Fredkin, Seth Lloyd, Thomasso Toffoli, Stephen Wolfram, and Konrad Zuse are some of the main contributors to this new direction.

JG: Anton Zeilinger pursues a similar position. In his article with Caslav Brückner they even note that "Quantum physics is an elementary theory of information". However, as one can expect, not all physicists share such a view of the physical world. A very strong criticism of such an information based view of the physical world has been recently expressed in a very angry article due to Daumer et al. in *quant-ph/0604173*.

CC: The first workshop "Physics of computation", organised at MIT in 1981, played a key role in understanding the role of information in physics and inaugurated the field of quantum information processing, communication and cryptography.

JG: It was the workshop organised by Thomasso Toffoli and of the topmost importance was the keynote talk of Richard Feynman in which he argued that classical computers cannot simulate efficiently quantum processes. This motivated David Deutsch to come in 1985 with a model of quantum computer—the quantum Turing machine. However, I think, Feynman could have hardly imagined how revolutionary this idea would be even for quantum physics.

CC: At that time quantum physics was considered deeply mysterious ...

JG: Indeed, Niels Bohr is often quoted to say that "Everybody who

is not shocked by quantum theory has not understood it." And even the same Feynman used to say, in 1965, in the introduction to his book *The Character of Physical Laws*: "I am going to tell you what Nature behaves like ... However do not keep saying to yourself, if you can possibly avoid it, 'but how can it be like that?' because you will get 'down the drain' into a blind alley from which nobody has yet escaped."

CC: The situation has changed nowadays, when a lot of hopes (and money) are put into quantum information processing.

JG: A new understanding of quantum world has already appeared by late 1980s. This was nicely summarised in 1990 by T. James who said: "Today we are beginning to realise how much of all physical science is really only *information, organised in a particular way.* But we are far from unravelling the knotty question: *To what extent does this information reside in us, and to what extent is it a property of Nature?* Our present quantum mechanics formalism is a peculiar mixture describing in part laws of Nature, in part incomplete human information about Nature—all scrambled up together by Bohr into an omelette that nobody has seen how to unscramble. Yet we think the unscrambling is a prerequisite for any further advances in basic physical theory." This, of course, does not mean that Feynman was wrong. We will never understand fully how can it be that nature behaves as it does.

CC: A better grasp of information and information processing could have a deep impact for our understanding of both the physical world and computer science, or, as you prefer, informatics.

JG: The impact on our understanding of the quantum world and physics is really significant. To start with, let us observe that in parallel to the algorithmic Church-Turing thesis since 1985 we have the physical Turing principle, formulated by Deutsch: *Every finitely realisable physical system can be perfectly simulated by a universal computing machine operating by finite means.* This principle can be seen as one of the guiding principles of physics. Today, we are witnessing an emergence of so many new views and approaches in quantum physics motivated mainly by results in quantum information processing. Some of them have strongly informatics background as the emerging NP-*principle*: "NP-complete problems are intractable in the physical world."

CC: What are actually the main contributions of quantum information processing and communication (QIPC) to (quantum) physics?

JG: They are numerous. On a very general level, QIPC should be seen as both an attempt to develop a new, more powerful, information processing technology, and as a new way to get deeper insights into the physical world, into its laws and limitations. QIPC gave rise to quantum informatics as the area of science combining goals and tools of both physics and informatics. QIPC is an area that brings new paradigms, goals, value systems, concepts, methods and tools to explore the physical world and its potential for information processing and communication is significant. On a more particular level, QIPC provides (quantum) physics with new concepts, models, tools, paradigms, images, analogies and makes many old concepts quantitative and more precise. In some cases, this even allowed to solve quite easily old problems. For example, an application of computability and complexity theories allowed to see that some old ideas about the physical world are wrong and that various proposals of modification of quantum mechanics are unlikely to work because they would allow the physical world to "easily" compute what is very likely beyond the classes **BPP** and **BQP**. Moreover, QIPC helped the understanding of phenomena that were considered for years strange and even mysterious, such as entanglement and non-locality. QIPC brought new measures allowing to quantify the power of various quantum resources and a deeper understanding of what can be and what cannot be distinguished and measured either exactly or approximately.

Moreover, as recently Barnum pointed out, the nature of information, its flow and processing, as seen from various operational perspectives, is likely to be the key to a unified view of the physical world in which quantum mechanics is its appropriate description, at least from certain points of view. Finally, I would like to mention the importance of various new concepts for quantum physics that started to be explored due to impulses from QIPC. They are related to attempts to see relations of entanglement to other physical resources and an analogy between classical probability distributions and density matrices. An exploration of such old concepts as POVM measurement got now a completely new dimension and brought far reaching implications. Finally, QIPC results brought new ways to use quantum phenomena for QIPC, not only through unitary operations, but also through adiabatic computations and, very surprisingly, through measurements only.

CC: Your list is really impressive. Could you explain, in simple terms, just one example?

JG: OK. Quantum entanglement, that is the existence of quantum states of composed quantum systems that cannot be decomposed into the states of subsystems, was for a long time considered a strange consequence of (an imperfect?) theory. Nowadays, there are already many books discussing this precious, though hard to create and preserve, information processing resource, its laws and limitations, and there are already a huge variety of measures of entanglement with deep informatics and physics interpretations.

CC: In this context you may wish to explain the one-way computation.

JG: In the so-called one-way computation one starts with a special entangled state, so-called cluster state, a source, and then one performs only one qubit measurements. The discovery that this is a universal way of doing quantum computation has been a big surprise. Perhaps even more surprising is the recent observation, see *quant-ph/0702020*, that one-way computation can be seen as a form of phase transition with the information about the solution being the order parameter. That led to the discovery of interesting analogies between thermodynamical quantities as energy, entropy, temperature, thermalisation, magnetisation, on one side, and computational quantities of one-way computation as entanglement, computational capacity, inverse time, computation and measurement.

CC: The existence (and ubiquity) of uncomputable numbers may suggest a (negative) answer to the old question "Can every observable be measured?" The existence of computable, but unfeasible problems brings new light on (quantum) physics.

JG: Correct, it was, for example, used by Lloyd and Abrams to show that non-linear quantum mechanics would allow to solve NP-complete problems in polynomial time.

CC: How can QIPC contribute to various foundational issues?

JG: One cannot say that contributions of QIPC to foundational issues have been already breathtaking. It is understood/believed that QIPC has some potential to contribute to old debates on various interpretations and their relations. Perhaps the main effort of QIPC was concentrated so far on the question "Why quantum mechanics?" with the goal of finding *natural*, information-theoretic, or even information-processing cast, axioms of quantum mechanics.

CC: Clifton, Bub and Halverson (2003) showed that one can derive quantum mechanics from the following three (negative) "axioms": no

superluminal communication, no broadcasting, and no unconditionally secure bit commitment. This suggests that quantum theory should be regarded as a theory of (quantum) information rather than a theory about the dynamics of quantum systems. Technically, it seems that the proof needs the assumption that quantum mechanics is formulated in C^*-algebra terms.

JG: Indeed, this has been demonstrated by an counterexample due to J. Smolin.

CC: On the other hand, the impact of QIPC on classical information processing and informatics does not seem to be so big.

JG: Yes and no or no and yes, depending on the angle you look at the problem. Surely, "classical informaticians" can keep doing their job, to a very large extend, without paying attention to QIPC. On the other side, there are fundamental results that should be included in the new textbooks. For example, we have now a new understanding what feasibility means—to be in the **BQP** class and not in the class **BPP**. In cryptography we have a new concept of security—unconditional security guaranteed by physical laws and a variety of views on security of bit commitment and its modifications. Even in the area of "programming" attempts to specify, reason and verify quantum systems bring new points of view. All these examples are at the fundamental level. On a more practical level, we have already classical results by R. de Wolf and S. Aaronson (to be discussed in more details later), that have been obtained using quantum tools, though not yet very many.

CC: Please cite an example.

JG: Ronald de Wolf showed, using a quantum argument, an exponential lower bound for 1-query locally decidable codes; he provided, using again a quantum argument, a simple proof of the best lower bound on the rigidity of Hadamard matrices. In addition, Scott Aaronson showed quite easily that the class **PP** is closed under intersection, what used to be a famous open problem, by showing that this class is identical to a new quantum complexity class **PostBQP**, an extension of the major quantum complexity class **BQP**.

CC: What we have been discussing so far seems to indicate a certain similarity, or at least an interesting relation, between the scientific goals of physics and informatics.

JG: My position is that the main scientific goal of physics is to study

concepts, phenomena, processes, laws and limitations of the physical world and the main scientific goal of informatics is to study concepts, phenomena, processes, laws and limitations of the information world.

CC: What is the information processing world? How different is it from the physical world?

JG: Of course I don't have a clear idea. However, physics does not have either an absolutely clear idea about the physical world and, in spite of that, it has been extremely successful in studying it and in producing beautiful, powerful and useful results. And so does informatics.

CC: Contrary to the digital physics view you seem to believe that these worlds are sharply distinct. Then, which of these two worlds is the most basic one, if any?

JG: It is too early to answer this question. We need a lot of research to explore the relations between basic concepts, principles and so on of these two worlds. However, it may be one of these eternal questions. Actually, this is the most likely development.

CC: An instance of the question regarding which of the two worlds—physical or informational—is more basic has actually been considered in the process of understanding the nature of quantum states: do they represent an objective physical reality, real physical objects, or do they have a subjective information character as a compendium of probabilities for the outcomes of potential operations we can perform on them?

JG: The information view of quantum states, as a description/compendium of our knowledge (or beliefs) concerning probabilities of the measurements outcomes, is on one side strange, all of us would like to have some physical reality behind. But, on the other side, it allows to see the collapse of quantum states at the measurement as something that does not contradict much our common sense view of measurement.

CC: Was QIPC able to contribute to perhaps one of the most fundamental question of the foundation of quantum mechanics: should we view quantum measurement from inside (from the point of view of the observer) or from outside of both observer and observed?

JG: I don't think too much, yet. However, QIPC theory developed a flexibility in moving between these two views by focusing on the role of information held (through entanglement) or obtained (through measurement).

CC: Let us switch the subject a bit. You have strong views concerning the relation between informatics and physics. How about the relation between informatics and mathematics?

JG: On the scientific level, I see mathematics as a part of informatics, as it used to be actually for centuries. In addition to being a science, I see mathematics as a basis of the so-called theoretical methodology that science has (as a complement to the experimental methodology) and I see informatics as the basis of a new, third, methodology of science. I even envision that our—so called Galilean science, where producing outcomes in a mathematical form was often seen as the main goal of the research—is quite fast developing to a new era of science, where results of our research are going to be much, much more demonstrated by "informatics products" such as simulation system, visualisation systems, algorithms and their analysis and so on, but also by studying virtual spaces. In other words, instead of trying to understand our world in mathematical terms, and in this way to make our findings available for future generations to utilise them, we will try, in future, to understand our world in informatics terms (that include, of course, all mathematical terms), and in this way to make them available for current and future generations to utilise them.

CC: Well, informatics didn't exist for centuries like mathematics ... I think few mathematicians would agree with you. One could argue, for example, that mathematics is not only about computation or information. Mathematicians have routinely studied non-computational mathematics, non-real, non-physical, many-dimensional spaces. In the last century we saw the transition between mathematics understood as calculation and mathematics considered as qualitative conceptual reasoning.

JG: Well, you have addressed several important issues and let me comment them briefly. First of all, informatics exists too for centuries and its origins are at least as old, if not older, as those of mathematics. Modern computers brought only a new dimension into many areas of the field—for example, an understanding of deep impacts of the study of various complexity problems and of the study of specification, reasoning and verification systems. Informatics is not only about computation and information. Far from that—as I have already mentioned, its main goal is to study, on the scientific level, laws, limitations, phenomena and processes of the information processing and to do that all useful tools are eligible. For example, I see Bourbaki's approach as very appropriate for their time—that is already over.

Concerning transitions mathematics went through, I would like to add that Halmos even said that applied mathematics is important, interesting, but bad mathematics. Until quite recently, mathematics saw computational and information processing mathematical problems also as interesting, important, but far from being "The Mathematics". Look, the book *Mathematical Thoughts from Ancient to Modern Times* (1200 pages on the history of mathematics) published in 1972 by Maurice Kline, does not contain a single occurrence of the term *algorithm*. It mentions al Chwarizmi, Turing, and even Babbage and many scientists behind modern informatics, but, clearly intentionally, avoids the term *algorithm*. This indicates to me how deformed was the mathematical thinking of that time (and, often, still is). On the other hand, neither all informatics deals only with problems directly related to information processing. In order to meet its long term goals, any science has often gone to abstractions, generalisations and models that are, at least at a first view, far from its original goals. In other words, I see nothing in the development of mathematics that would convince me that mathematics is not a part of informatics.

CC: Mathematical generalisations and abstractions turned out to be very powerful.

JG: Correct, but informatics goes much farther. It takes all generalisations and abstractions mathematics uses and adds many more, for example the study—by simulations in virtual or cyber-spaces—of such fundamental issues like quasi-biological processes. It demonstrates once more that visualisation has enormous discovering power.

CC: It won't be easy to make such a view acceptable.

JG: Well, some generations of mathematicians have to die out. But the process can be more straightforward. In connection with that I like to remember one story. At the reception of the World Computer Congress in 1989 in San Francisco I asked Donald Knuth, who was the main keynote speaker of the Congress, whether we should not do more to promote computer science. His response was, freely cited, that there is no big need to do something because in 50 years half of the members of Academy will have strong computer science background and support will come naturally. Now I believe, to make an analogy, that in 50 years half of mathematicians in Academy will be actually computer scientists and the development will go along the lines I have indicated.

In connection with that I have an idea. It could be a great contribution

to mathematics and informatics, and to science in general, to write a book about the history of mathematics with similar goals as the one of Kline, but demonstrating that the history of mathematics is a part of the history of informatics. And also to show that the main impact of mathematics thinking on the development of society came primarily through new computation (and information processing) methods and tools.

CC: How do you see the relation between informatics and mathematics in the future?

JG: I can imagine that in some places one will study mathematics as a special direction/sub-area within informatics departments. Actually, that would be very beneficial for both. In some places, we will have departments of mathematics in parallel with departments of informatics. This is similar to the current situation where we have in parallel departments of informatics, departments of statistics or operational research.

CC: Are you not going too far?

JG: I would like to go even farther. Mathematics departments have usually three goals: to service other sciences by preparing their students in mathematics, to bring up a new generation of mathematicians and to do research in mathematics. I start to be more and more convinced that informaticians, those theoretically oriented, could do the service I mentioned to other sciences better than (most of) mathematicians.

CC: Do you like to pursue even further your idea of (all) powerful informatics?

JG: Currently, science is divided into natural sciences, social sciences, technical sciences, agricultural sciences, liberal art sciences and so on. I envision the emergence of information sciences as another important area of science including: informatics (mathematics), technical informatics, bioinformatics, natural science informatics, economical informatics, educational informatics and perhaps such areas as entertainment informatics, geography, ...

CC: When you talk about informatics, it seems that you (mainly) have in mind theoretical informatics.

JG: Not really, but I like to see theoretical informatics as much broader area of science as it is mostly taken. Not only as the one where mathematical methods dominate. I expect that we will witness a similar

development with informatics as physics went through, where various branches of engineering developed from areas of physics.

CC: Do you believe that your view of mathematics as a part of informatics can be attractive to students?

JG: Of course. Look, mathematics does not actually have currently very big problems that would be attractive from outside. It surely has interesting and hard open problems, such as the Riemann Hypothesis, but one can hardly say that their solution would have a bigger impact outside mathematics. On the other hand, informatics has almost an infinity of extremely attractive challenges whose solutions could significantly influence mankind. For example, to create artificial brains, driver-less cars, to understand life, to find out whether our world is exponential or polynomial space, and so on—perhaps to make hard sciences from (some or many) soft sciences.

CC: Your picture of science raises many question ...

JG: Processes of differentiation and integration in science go often beyond all expectations (physics actually grew from medicine). In addition, the absolute truth is not always important; it may even not exist. What counts is whether a point of view is useful and can significantly contribute to the development of science (involved sciences).

CC: To explore the relations between the classical and quantum worlds is another challenge.

JG: Well, views on these two worlds can be very different. Niels Bohr said "There is no quantum world. There is only an abstract quantum physical description. It is wrong to think that the task of physics is to find out how Nature is. Physics concerns what we can say about Nature." A. Zeilinger noted "The border between classical and quantum phenomena is just a question of money." I find very interesting D. Greenberger's position who said "I believe there is no classical world. There is only quantum world. Classical physics is a collection of unrelated insights: Newton's laws. Hamilton's principle, etc. Only quantum theory brings out their connection. An analogy is the Hawaiian Islands, which look like a bunch of islands in the ocean. But if you could lower the water, you would see, that they are the peaks of a chain of mountains. That is what quantum physics does to classical physics."

CC: This is interesting.

JG: The search for such borders between classical and quantum worlds came recently to the experimental level. An important current research agenda is to find out for what kind of macroscopic objects such phenomena as superposition or entanglement hold. For example, these phenomena have been demonstrated already on an ensemble of 10^{14} atoms and on large molecules.

CC: Do you believe in Greenberg's position, or do you think that quantum mechanics holds only in certain parts of the physical world? Certainly your car mechanic is a classical mechanic, not a quantum one.

JG: Quantum mechanics surely brought a revolution in our view of the physical world. I would like to join those expecting that this revolution is not finished. One reason is that all attempts to get within this theory a unified understanding of time and space, cosmology and gravitation failed. One has therefore to admit that this is one of the reasons quantum mechanics is still not "the theory" of the physical world. Smolin, see *quant-ph/0609109*, has recently explored the hypothesis that quantum mechanics is an approximation of another, cosmological theory, that is accurate only for the description of subsystems of the universe. He found conditions under which quantum mechanics could be derived from the cosmological theory by averaging over variables that are not internal to the subsystem (and can be seen as non-local hidden variables of a new type).

CC: Should informatics get involved in such megastar problems?

JG: I even argue that this is one of the main challenges and tasks for theoretical informatics. These are really the *problems* theoretical informatics should try to deal with instead of being concerned so much with numerous attempts to close various $\log^* n$ and $\log \log n$ gaps, to say it metaphorically.

CC: This makes us to come to the question: what are really the main reasons to pursue quantum information processing and communication?

JG: On a common sense level, I see, as it was already mentioned, that QIPC is the result of a marriage between perhaps the two most important areas of science of 20th century: quantum physics and informatics. It would therefore be very surprising that such a marriage would not bring important outcomes for the whole science and technology. On a more technical level, I see the following reasons:

- QIPC is believed to lead to a new quantum information processing

technology that will have deep and broad impacts, on science, technology and society in general.

- Several sciences and technologies are approaching the point at which they badly need expertise with isolation, manipulation and transmission of particles.
- It is increasingly believed that new, quantum information processing based tools for understanding quantum phenomena can be developed.
- Quantum cryptography seems to offer higher levels of security and could be soon feasible.
- QIPC has been shown to be more efficient in interesting/important cases.

CC: May I observe that with the exception of the last "reason" everywhere else you have used terms like "it seems", "it is believed". Could you give us the simplest example of a *provable* QIPC solution which is more efficient than any classical solution (except Grover's algorithm)?

JG: Several: quantum teleportation cannot be made classically; if communicating parties share entanglement this may increase the capacity of their classical channel; in the area of quantum communication complexity, exponential separation has been proven for some problems. Finally, let me mention Simon's problem: Check whether a given finite function is one-to-one or two-to-one. In this case it has been proven, in a reasonable sense, that quantum solution is exponentially faster than any probabilistic solution—the weak point of this result is, however, that it is a promise problem and we work with query complexity.

CC: Deutsch's problem—test whether a bit-function is constant or not—was considered for many years the simplest example of a problem in which the quantum solution is superior to any classical solution; apparently nobody really checked this claim. In *quant-ph/0610220* I showed that classical solutions as efficient as the quantum one exist. Is any of the above listed examples in the same category?

JG: Your classical solution of the Deutsch problem has been a big surprise. People have realised that what has been claimed to be a more efficient quantum solution of the Deutsch problem is actually a solution of a different problem, with a different black box and inputs. It was only

believed that this is not something essential, but you have shown that it is. I tend to believe that this will not be the situation in the cases mentioned above, but I have to admit that I am not fully sure. Another surprising recent result along these lines is the recent discovery, *, quant-ph/0611156*, that Quantum Fourier Transform over $\mathbf{Z}_q$, which has been thought to be the key quantum ingredient of Shor's algorithms, can be simulated on classical computers in polynomial time. All that actually demonstrates how little we actually know about the computational power of quantum phenomena—entanglement, superposition and measurements.

CC: In connection with that, it is perhaps useful to mention that many solutions offered by quantum information processing make a crucial use of several hard to accept, counterintuitive phenomena as randomness of quantum measurement, the existence of entangled states and quantum non-locality. In some other cases, even more weird phenomena are used, for example, quantum counterfactual phenomena. Could we now turn our attention to them and perhaps start with quantum measurement.

JG: Results, both classical and quantum, of the basic quantum projection measurement should be random and should result, in general, in a collapse of the state being measured. Already Erwin Schrödinger had problems to accept it and his position is well known: "Had I known that we are not going to get rid of this dammed quantum jumping, I never would have involved myself in this business." Albert Einstein famous claim "God does not play dice" got a superb response from Niels Bohr: "The true God does not allow anybody to prescribe what he has to do." However, experiments seem to confirm randomness—summarised by Nicolas Gisin in his "God tosses even non local dices"—-to emphasise the existence of the shared randomness the quantum measurement of entangled states produces. Interestingly enough, physicists seem to have more problems to accept randomness than informaticians, because informatics has a lot of technical results showing the power of randomness for computation and communication. I would therefore like to say that *God is not malicious and provides us with useful randomness*. One should notice there are still very prominent old physicists and some bright young physicists having problems to accept randomness at quantum measurement. However, I have different problems concerning quantum measurement. A key step in some quantum algorithms is the measurement at which Nature finds, in a single step, for a given (actually any) integer function f, and randomly chosen y from the range of f, all x such that $f(x) = y$, and then incorporates

all such x into a superposition of basic states. I have really problems to believe it fully in spite of the fact that the mathematics behind it is perfect once we accept the principles of quantum projective measurement.

CC: Entanglement is even a more esoteric phenomenon.

JG: Again, mathematically the existence of entangled states is very easy to understand. However, if physical consequences are considered, the situation is different. Look, a very simple CNOT-gate should be able to process two independent particles in such a way that they get entangled and stay entangled no matter how far away they move. This is extremely hard to believe, though experiments (not really perfect) confirmed entanglement already among very different physical objects, as, for example, photons and atoms, and even for the distance of 144 km as recently demonstrated by Weinfurter's group in open space in Canary Islands—what has been a quite shocking recent experimental outcome. In addition, using the process called entanglement swapping, one can make entangled particles that have never been interacting.

CC: In spite of that entanglement is an important information processing resource.

JG: Some even say that it is a new gold mine of the physical world because entanglement allows to create such events, impossible in the classical world, as quantum teleportation, to create quantum algorithms that are faster than any known classical algorithm (for the same problem). Entanglement is a key tool to make some communications even exponentially more efficient than what one can classically achieve; to increase the capacity of communication channels; to act as a catalyst and so on. In addition, entanglement allows to create pseudo-telepathy. Asher Peres pointed out nicely that "entanglement allows quantum magicians to do things no classical magician can do".

CC: There are quite different views on entanglement.

JG: Indeed, entanglement has many faces. One can see it as a bridging notion between QIPC science and fields so different as condense-matter physics, quantum gravity and so on. There are various approaches to generalise this concept. A recent one is based on the idea that quantum entanglement may be directly defined through expectation values of preferred observables—without reference to preferred subsystem decomposition. Such a framework allows the existence of non-trivial entanglement within a

single indecomposable quantum system ...

CC: Possibly the most controversial issue concerning entanglement is the existence of non-local correlations created by a measurement of entangled states. Could we discuss this counterintuitive phenomenon in more details?

JG: Not many realise that "physics was non-local since Newton times with the exception of the period 1915–25", as recently Nicolas Gisin pointed out. In other words, since Newton's time the main physical theories implied the existence of non-local phenomena with the exception of the above period. In 1915, Albert Einstein came with the theory of relativity that denies the existence of immediate non-local effects, but quantum mechanics then brought certain non-local effects back into the mainstream physics.

CC: Newton himself had noticed counterintuitive consequences of his theory of gravity.

JG: Yes, for example, Newton realised that according to his theory if a stone is moved on the moon, then weights of all of us, here on the earth, are immediately modified. However, he actually believed that the reason is an imperfection of his theory. His words on this subject are very interesting: "That Gravity should be innate, inherent and essential to Matter, so that one Body may act upon another at a Distance thro a Vacuum, without the Mediation of any thing else, by and through which their Action and Force may be conveyed from one to another, is to me so great an Absurdity, that I believe no Man who has in philosophical Matters a competent Faculty of thinking, can ever fall unto it. Gravity must be caused by an Agent acting constantly according to certain Laws, but whether this Agent be material or immaterial, I have left to the Consideration of my Readers."

CC: Newton's observation may further complicate the attempts of losing weight ... More seriously, Leibniz criticised Newton's theory of gravity as a revival of the "occult properties" of medieval philosophy. However, quantum non-locality is different. It does not allow superluminal communication and therefore it does not contradict relativity. Did Einstein realise that? Can we have stronger correlations than those induced by entanglement without contradicting relativity theory?

JG: There have been many interesting recent developments in entanglement and non-locality. For example, Methot and Scarani in *quant-ph/0601210* pointed out that there are good reasons to consider

quantum entanglement and quantum non-locality as two independent resources. Namely, they have shown that for the main known measures of non-locality, not maximally entangled states are maximally non-local. However, the main new impulse for the study of non-locality came from the introduction of so-called PR-boxes by Popescu and Rohrlich, in 1997, in a paper that started to attract attention only fairly recently.

CC: The introduction of PR-boxes was an unexpectedly stimulating idea.

JG: They were intended as a toy tool that demonstrates (in a reasonable sense) a non-locality stronger than quantum non-locality which does not contradict relativity. PR-boxes are easy to describe. Indeed, a PR-box can be seen as consisting of two black boxes operated by two (very) distant parties that cannot have any direct communication. If one party, say A, puts on the input of its sub-box a (random) bit x_A, then it gets, immediately, as an output, a random bit y_A. The same for other party B. However, in spite of the fact that each of the inputs and outputs are random, the outputs should be always correlated with inputs as follows: $x_A \cdot x_B = (y_A \oplus y_B)$.

PR-boxes could be very powerful. Indeed, having enough of them we could have unconditionally secure bit commitment and, moreover, each distributed computation of a Boolean function could be done using only one bit of communication, something no one could believe. This quantum communication complexity result implies that PR-boxes cannot exist physically. This result was again one of the impressive contributions of the complexity theory to quantum mechanics.

CC: In spite of that PR-boxes keep being investigated.

JG: Yes, because they play a central role in the study of non-locality that does not contradict relativity theory. For example, an interesting question is how well we can approximate PR-boxes. It was shown that with shared entanglement one can approximate PR-boxes with success probability 0.854 and in no physical world this can be done with success probability of more than 0.908.

CC: Quite interesting! Counterfactual effects are other mysterious phenomena.

JG: I see them as another indication that something may not be OK in our understanding of the physical world. Counterfactual effects allow, for example, for the possibility to get the result of a quantum computation

without actually performing the computation. Recently, Paul Kwiat has presented the first demonstration of counterfactual computation using an optical-based quantum computer (see the Feb. 23 issue of *Nature*).

CC: A deeper understanding of all these phenomena is a challenge for physics.

JG: And for informatics too. There are of course many other very big challenges. Let me mention some of them: Is our universe computable? Efficiently computable? Is our world a polynomial or an exponential place? (As pointed out by Scott Aaronson.)

CC: Could our world be exponential?

JG: Well, without believing in exponentiality of our physical world we could have problems to explain some experiments already done. We do not consider as feasible a computation requiring exponentially growing number of steps, but no one actually seem to complain to have exponentially large probability distributions. The situation with exponentiality is therefore far from obvious and far from simple. As pointed out by Goldreich, we may need more realistic complexity models of quantum computations and, I think, also of communication.

CC: Can we really have a powerful quantum computer?

JG: This challenge is an important current research agenda for physics and informatics. Could it happen that quantum mechanics "breaks down" before factoring large integers? Landauer was perhaps the first sceptic and his statement "One will need more than rain to stop this parade" reflects feelings of his time, but these feelings keep coming back again and again.

CC: Why "quantum mechanics can break down before factoring very large integers"?

JG: There are many arguments. From the history of physics one can extrapolate that each theory has its limits and therefore one could expect that current quantum mechanics does not hold for too small and too large scales. Some believe that the size of measuring devices will have to grow exponentially. In addition, there are people believing that we cannot fight decoherence or theoretical results that claim that if the reliability of elementary gates and "wires" reaches a certain threshold, then quantum information processing can be done in any time and space distance, are wrong or improperly interpreted.

CC: On a more general level an important problem is that of feasibility in physics.

JG: Feasibility in physics was for a long time determined by the following statement of Dirac: "Can every observable be measured? The answer theoretically is yes. In practice it may be very awkward, or perhaps even beyond the ingenuity of the experimenter, to design an apparatus which could measure some particular observable, but the theory always allows one to imagine that the measurement can be made." Nowadays, it is obvious that this is not so. Theoretically, we can have quantum states with uncomputable amplitudes. It is therefore clear that not everything one can find in quantum theory is feasible in practice.

Informatics is already quite far in its attempts to develop important concepts of feasibility. It first realised that there are non-computable numbers and later that there are unfeasible tasks and hard to compute computable numbers. It seems to me that physics is still behind the goal to get a very reasonable concept of feasibility. And it is an important task for both physics and informatics to work on it.

CC: Dirac's idea was that unitaries and projective measurement in Hilbert space exist in Nature. The fact that there are uncomputable numbers and unsolvable problems can be seen as implying that not all unitaries and measurements can be constructed. Does it mean that they cannot exist in Nature?

JG: This is an interesting and fundamental question. I do not have a sharp view on this issue. Is the question about the existence of a different category than the existence of uncomputable numbers? I guess yes.

CC: Let us go back to the possibility of constructing universal quantum computers. This is a much discussed question. What do you think?

JG: First of all, it is far from clear whether we would really need them for usual computations. The number of cases they may be more efficient can be practically small. That can be seen from the fact that we still have relatively few impressive quantum algorithms. A need for a general purpose quantum computer is therefore questionable. Another issue is the need to have powerful quantum special purpose processors or devices to simulate quantum phenomena and processes. To make a long story short, I believe that either we will have quantum computers or we will discover some new important limitations of the physical world.

CC: This brings us to the controversial issue of interpretations of

quantum theory. There are various sophisticated interpretations and a lot of articles have been written on this issue by scientists and philosophers of science.

JG: I think that there is a sophisticated mess concerning interpretations. I like the observation that not only philosophers of science cannot agree on a particular interpretation, but they have even a problem to agree on what is an interpretation.

On the other hand, I believe that outcomes of quantum informatics, especially in the area of quantum computation and communication theory, but also in cryptography, broadly understood, can bring more light into various interpretations and into the relations between them.

CC: By the way, how did you get involved in quantum information processing?

JG: In 1989, after being appointed as chairman of the newly created IFIP Specialist Group on Foundations of Computing (SGFCS 14), I worked out a very ambitious, and idealistic, program how SGFCS 14 could support the development of TCS. One of my suggestions was to create a working group Informatics and Physics. No one complained, but such an idea turned out to be too much ahead of time. In 1992 and 1993, during my three years stay at the University of Hamburg, I run, together with Manfred Kudlek, a physicist by education, a seminar "Informatics and physics". One of the papers we discussed was Deutsch's paper where the model of quantum Turing machine was introduced ... To make a long story short, in 1997–99 I wrote, partly on the beach in Nice, my book *Quantum Computing*.

CC: Could we now discuss the relations between physicists and informaticians. My first question is what should informaticians learn from physicists?

JG: I see three main directions: (1) physics sells itself better and in a more mature way; (2) physics is better organised; (c) physics has a better and mature publication policy.

CC: Of course, physics is much older than modern informatics.

JG: Correct, but still differences concerning the quality of selling are enormous. The main impulse for enormous support for physics came from the needs of the Second World War, and later of the cold war. Informatics has made in the last 50 years arguably larger contributions to science and society, but still the amount of money going into physics is much larger

than the amount informatics gets. I think physics leaders have realised that the society support of science is not mainly due to the fact that it brings important outcomes, but that generates mysterious problems and phenomena and solves some of them. Physicists have made some great marketing moves as making one of their goals to create a *theory of everything* (S. Hawking). Who could really believe in it? But this idea brought much support for physics in general and in UK in particular.

CC: Ignoring age, do you see any specific reasons why informatics is not as well organised as physics?

JG: Informaticians should start to understand that the way a field performs as the whole depends not only on how many clever young people it has, but even more on how many wise people it has in its leadership. The current value system in informatics, with such emphasis on accepted papers at "prestigious conferences", prefers young bright people and even the middle generation is very soon "out". This seems to be true especially in theoretical informatics. As a consequence, the field is scientifically doing very well, concerning solving hard open problems, but far less in the attempts to attack important new problems of the field and of science in general. The overall standing of theoretical informatics within the informatics community is quite low and goes actually down, quite fast, I think. Those that should be and could be leaders are put much too soon aside. Everybody in the field is then paying for that, in long terms.

CC: It seems that an emphasis on 3-4 page long papers dominates the publication policy in physics ...

JG: From the point of view of physics that was a clever idea. It is now embraced by a large number of authors. By writing two pages a scientist can have 10 publications (with 10 authors each) and if each such paper is cited, then physics has 100 citations. I am a bit dramatising situation, but not essentially. In any global evaluation of sciences, physics (and other natural sciences) dominate, to a large extend due to such publication policy, and, as a consequence, their interests dominate the current science in spite of the fact that the global interests of society would need to put the focus to other areas of science.

CC: Since there are now large possibilities for electronic publishing, informatics should be a leader.

JG: But it is not, and it is getting, again, far behind physics. Look

how much (and how cleverly) physicists use the Los Alamos archive. However, this is not all. Informatics clearly needs a more mature publishing policy. The current publishing policy in informatics, inherited, to a very large extend, from mathematics, is not well suited for informatics. As a consequence, once the number of publications, citations and impact factors start to be counted, informatics looks like performing not so well than areas of science with arguably smaller current impact on science, technology and society.

CC: On the other side, what physics can learn from informatics?

JG: On a very general level, one can say that informatics offers for (quantum) physics paradigms, concepts, and results that can allow physics to see sometimes faster what is impossible, to formulate and to sharp better results and to see deeper into the physical world.

One can say that quantum information processing concepts, paradigms, models and results forced physicists to reshape their ideas of reality, to rethink the nature of things at the deepest level, to revise their concepts of position and speed, their notion of cause and effect, ...

CC: And what physicists should learn from informaticians?

JG: Many things. In the area of quantum information processing, the use of the big-O notation to express scalability and feasibility. Then, an understanding that after learning an issue for small cases one should try to understand the general case, and to replace hand-waving arguing by precise proofs. Physicists are starting to learn that using complexity-theoretic models and results one can learn that certain phenomena are (likely) impossible and to understand the power of various quantum information processing resources, as entanglement, and non-locality.

One should realise that informatics has brought new views on old phenomena, and that is perhaps its main contribution.

CC: Complexity theory seems to be the main area of theoretical informatics physicists may find useful ...

JG: Correct. One can even say that the main reason why already von Neumann did not come with the idea of quantum information processing was the fact that in his time science couldn't see that quantum information processing would pay off. It was mainly due to (quantum) complexity results that made clear that quantum computing could pay off. Moreover, the main killer-applications for the whole field were actually Shor's algorithms

motivated by (quantum) structural complexity results.

However, I believe that other areas of theoretical computer science can significantly contribute to our understanding of the physical world. For example a recently emerging *quantum programming, specification and reasoning theory.*

CC: What else in informatics may be useful to physicists?

JG: For an informatician it is almost shocking the level of referencing in physics. For example, they do not write titles of the articles in references and the paper size (last page), though this is often a very important information.

CC: There has to be a reason for that.

JG: As I see it, a well-done dissemination of knowledge is still not the main goal of publications in physics as it is in informatics. The main goal of the whole publication system in physics seems to be a fast documentation of the priority of new discoveries. Physics was for centuries influenced by goals and customs that dominated when the science started. I think most of physicists even do not realise what is behind the rules that are imposed on them by journals and their publication culture. The emphasis on ensuring the priority of authors as the main goal of publications has as a consequence the fact that papers are (actually have to be) written in such a way that they are not easy to be read, checked and understood. This does not seem to be desirable. The main goal seems to be able to say (for authors): I was (we were) first to do that and that, it was published in ... Another goal of such publications, again inherited from old times, seems to prevent, as much as possible, the reader to make very fast use of the published results. One can say that physics papers are, at least to a large extent, "readers-unfriendly". The younger generation of physicists started to be different. While they may not realise why the publication policy is as it is, they still do not have enough power to change long time ago established policies and traditions. However, I should notice that a similar publication policy was used in former Soviet Union in mathematics. Easy to read papers had small chances to get accepted. Authors were under pressure to establish heavy formalism and to compress the paper as much as possible.

CC: I see this kind of tendency in many papers in theoretical computer science ...

JG: This is true, but this is more due to the abstraction the field goes into, the difficulty to describe informally formal systems and reasoning

about them. Fortunately, nowadays we do not depend so much on powerful editors. You can just put the complete version on your web page. Moreover, journals compete (and put prices) for best papers, ...

CC: Are the two communities of quantum information processing, one coming from physics and one coming from informatics, getting closer?

JG: Significantly, and I think that many physicists in QIPC have started to fully realise the power of informatics methods, and use them. (Actually, I do not know any other area of science, where TCS outcomes would be so useful and had such big impacts as in QIPC. QIPC can be seen as a really big success story of TCS.) Informaticians have started to appreciate the importance of many related theoretical problems of physics.

CC: Many have the feeling that after a big boom during 1993–96, the progress in the area of QIPC has been recently far less spectacular. Is it true?

JG: Comparing with 1994, the number of papers submitted to quantum archive has increased more than 10 times. This characterises pretty well the increase of the research in this area. Both theory and experiments have made an enormous progress. Theory results seem to be more technical and less spectacular. Experimental results, especially in quantum cryptography, may not be spectacular for a non-specialist, but for experts it has been achieved recently far more than one could have expected 10 years ago. For example, the first experiment in quantum cryptography was based on the transmission of photons for a distance of 32.5 cm. Nowadays the maximum is approaching 200 km, when fibres are used and was done for 27 km, from one peak to another, in Alps, and for 144 km, from one island (La Palma) to another (Tenerifa), via an optical free-space link. Some foresee even transmission to 1000 km using quantum repeaters. Hardly someone could have believed in such achievements 10 years ago. Experimental cryptographic networks, for example the DARPA network in Boston, are remarkable achievements.

CC: The situation seems to be very different in the attempts to design more powerful quantum processors. Factorisation of the number 15, and an experiment with 8 qubits, are still the most publicised results and that is far from being impressive.

JG: It is correct that impressive results in this direction are missing. The field is in the process of exploring various technologies and searching for various primitives and from this point of view the field is in cumulating state

of knowledge, methods and experience. There have been many surprising outcomes, as, for example, an understanding that quantum computation can be performed by measurements only, or the idea of one-way computing. It is true that there are still many pessimists not believing that we can win our fight with decoherence. However, while progress in science is often done by pessimists, progress in technology is always done by optimists. I like to remember the famous story of the Colossus, of our first really powerful electronic computer, designed by Tommy Flowers, in a post office laboratory, in spite of the fact that his proposal was rejected by a panel of experts as unfeasible. He did that because he knew that thermionic valves are reliable provided they are not turned on and off too often.

CC: Could a discovery of a simple technology make a miracle for quantum computing?

JG: Who knows, I believe so, I am an optimist.

CC: It takes a long time until new ideas make a real impact.

JG: Of course. For example, in the development of the last three centuries we can notice, from the science and technology point of view, the following common scenarios:

19th century was mainly influenced by the first industrial revolution that had its basis in the classical mechanics discovered, formalised and developed in the 18th century.

20th century was mainly influenced by the second industrial revolution that had its basis in the electrodynamics discovered, formalised and developed in the 19th century.

21th century can be expected to be mainly developed by quantum mechanics and informatics discovered, formalised and developed in the 20th century.

To summarise, it used to take about a century for new discoveries in science and technology to have a decisive and global impact on the society developments, and usually in a way no one could image at the very beginning.

CC: We have started our discussion with an observation that the concept of information plays such an important role nowadays for physics and our understanding of the physical world. A similar situation may apply

to the security and related cryptographic concepts.

JG: Indeed, I am expecting, more and more, that basic cryptographic (in a broad sense) concepts will play a very important role in our understanding of both information processing and physical worlds. They may play an even more important role (than the concepts related to information processing and transmission themselves) in our understanding of the laws and limitations of the physical and information worlds. Moreover, the impact of cryptography, again in a broad sense, goes fast even much farther. Growing needs to provide security, privacy, anonymity and authentication, especially in connection with one of the "ultimate, and never fully reached, goals of science and technology"—the design of global computation and communication networks, called usually grid networks, will create big and important specialised industries. This can be even one of the important driving forces of many industries and of the overall development of society.

CC: You seem to have again a very strong position ...

JG: I would also like to foresee, as another important area of science and technology, the emerging security science and technology. A science not only for security providing technologies, but as a really fundamental science. And not only that.

It is well known that history of mankind can be seen, in a very simplified form, as consisting of the following three eras. Observe that their descriptions differ basically only by one word. The three magic words are **food**, **energy** and **information**.

Neolithic era: Progress was made on the basis that man learned how to make use of the potentials provided by the biological world to have **food** available in a sufficient amount and whenever needed.

Industrial era: Progress has been made on the basis that man has learned how to make use of the laws and limitations of the physical world to have **energy** available in a sufficient amount and whenever needed.

Information era: Progress is and will be made on the basis that man learns how to make use of the laws and limitations of the information world to have **information** available in a sufficient amount and whenever needed.

In this context the following question arises: What can we expect to have as "being" in the fourth era to come? Of course, this is hard to

predict. *Artificial* (worlds, intelligence, life,...)? That may be the case, but I would like to foresee the fourth coming era as one in which the key concepts are those of security, safety, privacy, anonymity and so on. Modern cryptography, broadly understood, is the key science behind.

CC: How do you see modern cryptography?

JG: The general goal of modern cryptography is the construction of schemes which are robust against malicious attempts to deviate from a prescribed functionality. The fact that *an adversary can devise its attacks after the scheme has been specified* makes the design of such schemes very difficult—schemes should be secure under all possible attacks. It makes very difficult to specify precisely enough when a cryptographic scheme is perfectly secure.

CC: We have several concepts of security.

JG: Correct: informational security—an enemy has not enough information to break the scheme; computational security—an enemy cannot have enough computational power to break the scheme and so called unconditional security—an enemy cannot break the scheme, due to physical laws, no matter how much computational power she has.

CC: How successful is actually our "fight" for security?

JG: In this area we have a constant fight between "good" and "bad". Both sides are trying to (maximally) use whatever sciences and technologies bring us. Adi Shamir said that concerning security *we are winning battles, but losing wars*. One of the key issues is that society has still problems to realise and accept that security is very costly, requires sophisticated tools, and we have to pay for it with time and freedom.

CC: Why the study of security would lead to deeper issues into information processing and physical worlds?

JG: Look, in all problems concerning security, authentication, but especially concerning more subtle problems of anonymity and privacy, we have as goal to get *perfect* or *unconditional* security, anonymity, privacy, authentication and such a goal is much more demanding than to have more efficient computation or asymptotically best computation.

CC: Already well-known fundamental cryptographic concepts, as one-way function, one-way function with trapdoor, hard predicate, zero-knowledge proof, are fundamental for information processing.

JG: In addition, look how stimulating the study of variations of bit commitment, coin tossing and oblivious transfer protocols, has been for our understanding of the quantum information processing world and its relations to the classical information processing world.

CC: Please highlight a simple result in quantum cryptography.

JG: Unconditionally secure generation of classical keys and the impossibility of having unconditional secure bit commitment are theoretical highlights. However, even more surprising, at least for me, is that using a simple quantum version of a one-time pad cryptosystem one needs only two bits to hide perfectly any qubit even if its specification requires infinitely many classical bits.

CC: How about relations between cryptographic concepts and foundational issues of quantum mechanics?

JG: One of the big things of interest to foundational people is whether we can derive quantum mechanics from some simple axioms that have a natural physical, or information processing based, interpretation. Fuchs and Brassard suggested to consider as axioms (a) the existence of unconditionally secure cryptographic key generation, and (b) the impossibility of secure bit commitment. One such attempt was done, as I have already mentioned last time, by Clifton, Bub and Halvorson with three axioms: No signalling, no broadcasting, and no bit commitment.

CC: At a first glance, it seems odd that quantum mechanics could be derived from the axioms (a) and (b).

JG: Actually, it is not. Look, unconditional secure key generation is possible only if the no-cloning theorem holds and quantum measurement causes a disturbance of quantum states. Unconditionally secure bit commitment is impossible only in case we have correlations similar to those quantum entanglement provides. And here we are.

CC: We can therefore expect interesting developments at the intersection between informatics and physics.

JG: Of course, and at the end of our discussion I would only like to mention several citations to illustrate how the views of the physics and physical world keep changing. Demokritos is quoted as saying (400 BC) *Nothing exists except atoms and empty space; everything else is opinion*; Ernest

Rutherford said in 1912, *All science is either physics or stamp collecting.* My position is that *Physics is not the only science capable of producing a deep understanding of physical world. Informatics can and should help. Or, even, it should take the initiative.*