Very Digital Person: FAISAL SHAH KHAN

Quantum Computing (QC) brings a lot of hopes and new perspectives. When will QC replace our conventional smartphones, laptops and tablets?

To reach this stage of quantum ubiquity, a thorough understanding of how to interface conventional and quantum computational processes is needed. This is because any useful quantum computer has to be programmable. But this is a difficult task because the quantum realm is fickle, and objects in it decohere almost instantaneously upon interaction with the realm of conventional devices and programmers. Imagine trying to pass a thread through the head of a needle the size of a dust particle. Programming a quantum processor is orders of magnitude more challenging. But just like one can further imagine splitting the thread into finer and finer strands until reaching a strand thin enough to pass through our miniscule needle head, so can one imagine layers of physical processes starting with one that is conventional but with each additional layer transitioning toward the quantum realm. Ultimately, one imagines a layer of physical processes that bridge the quantum and classical realms. The collection of these processes serves to interface the classical programmer and the quantum computer. Quantum computing will replace conventional devices such as laptops and smartphones when scientists and engineers fully understand the interface of quantum and classical computational realms.

Where are we today in QC's development path? What are some current problems? Which kinds of problems do you work on?

The current stage of development of Quantum Computing is roughly similar to the stage at which conventional computing was during and immediately after the 2nd World War. This was the time of massive computing machines like the ENIAC (Electronic Numerical Integrator and Computer) and the MANIAC (Mathematical Analyzer Numerical Integrator And Computer Mode) which would take up large rooms to fit, but which would calculate solutions to only the simplest of problems. This is also the situation with respect to the current, first generation of quantum processors, which also physically take up large spaces but can only solve a small class of problems or problems of simple nature. This is largely due to the heuristic philosophy that has driven the development of this generation, which has left open problems relating to fully optimizing its development and performance. For Quantum Computing to evolve into a more efficient next generation, it is essential that the lessons learned from the efforts put into developing current Quantum Computing platforms be cast into formal mathematical machinery such as algebraic geometry, differential geometry, and topos theory. And these same lessons, combined with the insights gained from the mathematical machinery they are cast unto, must be used to foster developments in physics and materials science and engineering so that platforms for the next generation of Quantum Computing are closer to realizing the full potential of this technology.

"The current stage of development of Quantum Computing is roughly similar to the stage at which conventional computing was during and immediately after the 2nd World War."

I approach the problem of optimizing the next generation of Quantum Computing from a differential geometric point of view. More specifically, I am interested in the work of the late Nobel laureate John Nash. While Nash is more famous for his work in game theory where he developed the notion of Nash equilibrium, it is his work on the isometric embedding of Riemannian manifolds (the model for Quantum Computing) into Euclidean spaces (the model for conventional computing), that interests me. In particular, I want to understand Nash's embedding as a solution to the problem of interfacing quantum and conventional computing paradigms, with specific focus on:

i) Fabrication of hardware architectures that perform Quantum Computing, but which necessarily reside in Euclidean space.
ii) Understand what firmware for quantum computing is required.
iii) Develop robust cyber-security protocols resistant to Quantum Computing attacks.

Other mathematically formal approaches I am pursuing in this context include non-commutative geometry, topos theory, and a theory of fixed-points in the quantum computational domain. The latter is interesting to me because it may allow the application of Nash's Noble prize-winning work on equilibrium in games to constrain-optimize the performance of quantum processors.

After having solutions, what are the future major impacts of QC?

Let me start with the Nash equilibrium. In strategic interactions between "players", Nash equilibrium is an outcome that no player wishes would change. In other words, given the strategic choices made by all the players, Nash equilibrium is an outcome of the interaction where each player is most satisfied. This idea serves as a solution concept in many applied areas, including economics, computer science, evolutionary biology, and politics. As ubiquitous as its usefulness is, the problem of calculating Nash equilibrium outcomes in interactions with a large and practically meaningful number of players is computationally intractable for conventional computing. The ability to quickly solve for

Nash equilibrium using Quantum Computing will have a dramatic effect on all areas of strategic decision making, with finance, politics, and biological sciences potentially being revolutionized due to the fundamental role Nash equilibrium plays in these fields.

Another major impact would be on computing solutions to problems in fundamental sciences. This was the idea behind Richard Feynman's original proposal for a quantum computer, where the properties of a complicated quantum physical or chemical system were simulated on a simpler one which was easier to control. This allowed quick solutions to problems that were intractable using conventional computers. Consider for instance the problem of water desalination (or water purification in general). While membrane technologies using the idea of reverse osmosis exist and function efficiently from several practical points of view, it is nonetheless fruitful to ask what the minimal energy for separating the molecules of salt and water is. Quantum computing can answer this question. When combined with techniques in artificial intelligence, a quantum computer can be trained to calculate the separation efficiency as a function of the molecular components. Resulting insights have the potential to make current and future desalination technologies socio-economically optimal by suggesting the feasibility of any separation process on the basis of the thermodynamic barrier for molecular separation.

Is the quantum computer a risk for our conventional security keys?

Yes, absolutely! Especially those security keys that are constructed using prime number multiplication and taking discrete logarithms. These two mathematical procedures, which have formed the backbone of secure key generation for the past several decades, have been conclusively shown to be trivial to break using a sufficiently large and fully functioning quantum computer. While the current first generation of quantum computers is not a threat to security keys, I imagine that this threat would be very real within a decade, and maybe even less. However, several methods have been forwarded to thwart Quantum Computing attacks on security keys, and these include making keys using alternative mathematic methods such as lattices, or using the quantum physical phenomenon of ideal randomness that even a quantum computer cannot discern patterns in.

"So while somewhat indirectly connected to the question of Quantum Computing and computer games, this discussion points to another improvement Quantum Computing can offer to the theory of games in general."

What's the connection between QC and the modern computer game?

There are two perspectives I would like to give here. The first one deals with graphical representation and image resolution. In modern computer games, three-dimensional features and motion are depicted onto a two-dimensional screen. This dimensionality reduction is not so much the problem as is the Gimbal lock, a situation affecting rotations in three-dimensional space where one degree of freedom is lost. The Gimbal lock manifests in computer graphics as an abrupt, discontinuous motion that is aesthetically unpleasant and which can adversely affect the user experience. The way to avoid Gimbal lock in computer graphics is by first representing three-dimensional rotations as four-dimensional objects known as quaternions, and then projecting these quaternions into the two-dimensional graphics space. The result is a smooth, continuous motion in two dimensions that may in fact enhance the user experience beyond what is experienced in reality.

The connection of all of this with Quantum Computing becomes clear when one notes that an important subset of the quaternions, the unit quaternions, is in fact mathematically equivalent to Quantum Computing! In other words, when one enhances two-dimensional computer graphics using quaternionic algebra, in effect, one is simulating a quantum computation on a conventional computer! Given that conventional computers have limited capacity in simulating quantum computations, one can only imagine the enhancement to computer graphics that can result from interfacing this process with an actual quantum computer.

The other perspective relates to the topic of Nash equilibrium that I mentioned earlier. Board games and computer games are entertaining because their makers either ensure that at least one player wins, or they try to build an interesting Nash equilibrium outcome. Take Tic-Tac-Toe for example; either one player wins this game, or both players end in a draw, which is a Nash equilibrium. However, this is hardly an interesting equilibrium outcome. What scientists studying the theory of "quantum games" have shown is that if a conventional game is enhanced using quantum computational techniques, then enhanced and interesting Nash equilibrium outcomes manifest. For example, in the famous game of Prisoner's Dilemma, where a pair of conspiring thieves are arrested and interrogated by police in separate rooms, the Nash equilibrium outcome is one where each thief implicates the other and spends the maximum amount of time in jail. This situation can be im-

Faisal Shah Khan

Faisal Shah Khan currently serves as an Assistant Professor of Mathematics and Principal Investigator in the Center on Cyber-Physical Systems at Khalifa University, Abu Dhabi.

He has a PhD in Mathematical Sciences from Portland State University, earned under the supervision of Professors Steven Bleiler and Marek Perkowski.

Khan has supervised graduate and undergraduate students on projects involving Quantum Computing, imaging, and non-cooperative game theory.

His research work involves studying the Nash embedding theorem, using differential geometry as a mechanism:

a) for developing programming paradigms that will allow a classical programmer to program a quantum computer, in a mathematically and physically robust way.

b) for identifying fixed-point stability in quantum games with applications to locating equilibrium and optimal performance of quantum computations.

proved upon in a quantum mechanical version of the game. So while somewhat indirectly connected to the question of Quantum Computing and computer games, this discussion points to another improvement Quantum Computing can offer to the theory of games in general.

Is there a connection between QC and artificial intelligence?

I will refer here to the persuasive work of Johnjoe Mcfadden and Jim Al-Khallili's. These two physicists consider quantum physical effects like entanglement and measurement to have played an indispensable role in the development of life, its evolution, and the emergence of consciousness. If quantum physics can play a role in the development of a higher order of natural intelligence, that is, consciousness, then I don't see why quantum computation would not play a fundamental role in the development and emergence of the much simpler notion of artificial intelligence.

A glimpse at the future: what is your vision of a quantized world?

The science fiction icon, Isaac Asimov, proposed the idea of computers and robots with artificial consciousness all the way back in the 1950's. In fact, two robotic protagonists in his novels consciously conspire to bring about the development of humanity as a galaxy-faring species. Unlike conventional electronics even back in the 1950's, Asimov's robots had brains that processed positrons instead of electrons. I have decided over the years that this was Asimov's way of expressing his premonition of quantum computers! But he more accurately expressed his vision of a quantized future in a short story titled *The Last Question*, where he envisioned generations of humanity and the artificially intelligent computers it builds, evolving in tandem until the computer and its creators merge into one, giving the computer sentience, and ultimately, a form of godhood.

While I share Asimov's vision of a future quantized world, I like to think that I am a bit more conservative. I certainly feel that Quantum Computing will play a crucial role in the development of fast and accurate artificially intelligent agents that may also evolve a certain level of consciousness. But unlike those who predict a Skynet-style termination of the human species due to AI, I like to think that conscious AI will be benevolent. For consciousness is an essential pre-requisite for the development of culture, and a culture requires, at the very least, a selfishly-motivated concept of altruism to be successful. I think AI and QC will be abundant in the quantized world of the near future, and that this will produce a wonderful and bright future for humanity.

"I certainly feel that Quantum Computing will play a crucial role in the development of fast and accurate artificially intelligent agents that may also evolve a certain level of consciousness."

Interview: Hannes Mittermaier

Photo: personal