Hybrid Quantum Computing Apocalypse

Robert Skopec

1De Dubnik, Researcher-analyst, Slovakia

Correspondence: Robert Skopec, Dubnik, Slovakia, Researcher-analyst, E-mail: zxcbnvm7@gmail.com

Received: July 30, 2018 Accepted: August 10, 2018 Online Published: August 22, 2018

Abstract

Chinese scientists won a major victory, by proving that the Majorana fermions – a particle we’ve found tantalizing hints for years – genuinely exists. This discovery has huge implications for quantum computing, and it might change the world. Don Lincoln, a senior physicist at Fermi lab, does research using the Large Hadrons Collider. He is the author of “The Large Hadrons Collider: The Extraordinary Story of the Higgs Boson and Other Stuff That Will Blow Your Mind”, and produces a series of science education videos. To the question: Why is there (in our Universe) something including cancer, rather than nothing? He is giving the simplest scientific answer: We shouldn’t exist at all.

Keywords: Hybrid, Quantum, Computing, Apocalypse, Multiverse.

1. Multiverse Theory and Dark Energy

Each universe in a multiverse contains different levels of dark energy, according to the dominant theory. A hypothetical multiverse seems less likely after modeling by researchers in Australia and the UK threw one of its key assumptions into doubt. The multiverse concept suggests that our universe is but one of many. It finds support among some of the world’s most accomplished physicists, including Brian Greene, Max Tegmark, Neil deGrasse Tyson and the late Stephen Hawking. One of the prime attractions of the idea is that it potentially accounts for an anomaly in calculations for dark energy.

The mysterious force is thought to be responsible for the accelerating expansion of our own universe. Current theories, predict there should be rather more of it around than there appears to be. This throws up another set of problems: if the amount of dark energy around was as much as equations require – and that is many trillions of times the level that seems to exist – the universe would expand so rapidly that stars and planets would not form – and life, thus would not be possible.

The multiverse idea to an extent accounts for and accommodates this oddly small – but life permitting – dark energy quotient. It permits a curiously self-serving explanation: there are a vast number of universes all with differing amounts of dark energy. We exist in one that has an amount low enough to permit stars and so on to form, and thus life to exist.

So far, so anthropic. But now a group of astronomers, including Luke Barnes from the University of Sydney in Australia and Jaime Salcido from Durham University in the UK, has published two papers in the journal Monthly Notices of the Royal Astronomical Society that show the dark energy and star formation balance isn’t quite as fine as previous estimates have suggested. The team created simulations of the universe using the supercomputer architecture contained within the Evolution and Assembly of GALaxies and their Environments (EAGLE) project. This is a UK-based collaboration that models some 10,000 galaxies over a distance of 300 million-light years, and compares the results with actual observations from the Hubble Telescope and other observatories. The simulations allowed the researchers to adjust the amount of dark energy in the universe and watch what happened. The results were a surprise. The research revealed that the amount of dark energy could be increased...
a couple of hundred times – or reduced equally drastically – without substantially affecting anything else. For many physicists, the unexplained but seemingly **special amount of dark energy in our universe is frustrating puzzle.** Above simulations show that even if there was much more dark energy or even very little in the universe then it would only have a **minimal effect** on star and planet formation. This implies that **life could potentially exist in many multiverse universes.**

The multiverse was previously thought to explain the observed value of dark energy as a **lottery** – we have a lucky ticket and live in the universe that forms beautiful galaxies which **permit life** as we know it. Cited works show that our ticket seems a little too lucky. It’s **more special than it needs to be for life.** This is a problem for the multiverse, a puzzle remains.

It is a puzzle that goes right to the heart of the matter: if the dark energy assumptions are flawed, does a multiverse even exist? The formation of stars in a universe is a **HYBRID battle between the attraction of gravity, and the repulsion of dark energy.** So **why such a paltry amount of dark energy in our universe?**

Probably, we should be **looking for a new law of physics** to explain this strange property of our universe, and the multiverse theory.

**2. Why the Universe Shouldn’t Exist at All?**

Don Lincoln, a senior physicist at Fermilab, does research using the Large Hadron Collider. He is the author of “The Large Hadron Collider: The Extraordinary Story of the Higgs Boson and Other Stuff That Will Blow Your Mind”, and produces a series of science education videos. To the question: Why is there (in our Universe) something including **cancer,** rather than nothing? He is giving the simplest scientific answer: We shouldn’t exist at all.

Give some scientists 65 pounds of rare isotope of germanium, cool it to temperatures cold enough to liquefy air, and place their equipment nearly a mile underground in an abandoned gold mine, and you’ll have the beginnings of an answer. Their project is called **the Majorana Demonstrator** and it is located at the Sanford Underground Research Facility, near Lead, South Dakota.

To grasp why science has trouble explaining why matter exists – and to understand the scientific achievement of **Majorana** – we must first know a few simple things. First, our Universe is made exclusively of matter, all people, the Earth, even distant galaxies. All of it is matter.

Our best theory for explaining the behavior of the matter and energy of the Universe contradicts the realities that we observe in the Universe all around us. This theory, called **the Standard Model,** says that the **matter** of the Universe should be accompanied by an identical amount of **antimatter,** which, as its name suggests, is a substance **antagonistic to matter.** Combine equal amounts of matter and antimatter and it will **convert into energy.** And the street goes both ways: **Enough energy can convert into matter and antimatter** (since antimatter’s discovery in 1931).

Modern cosmology says the Universe began in an unimaginable **Big Bang** – an explosion of energy. In this theory, **equal amounts of matter and antimatter should have resulted in cancer.** So how our Universe made exclusively of matter? However, we don’t know the process whereby **the asymmetry in the laws of the Universe arose.** One possible explanation revolves around a class of subatomic particles called **leptons.**

The most well-known of the leptons is the familiar **electron,** found around atoms. A less known lepton is called **the neutrino. Neutrinos** are emitted in a particular kind of **nuclear radiation,** called **beta decay.** It occurs when a neutron in an atom decays into a proton, an electron, and a neutrino. Neutrinos are fascinating particles. They interact extremely weakly, a steady barrage of neutrinos from the nuclear reactions in the Sun pass through the entire Earth essentially without interacting.

Still a mystery to scientists is whether there is a difference between neutrino matter and neutrino antimatter. While we know that both exists, we don’t know if they are different subatomic particles or if they are **the same thing.** We don’t know which kind of twins **the neutrino matter/antimatter pair** are. If **neutrinos are their own antimatter particle,** it would be an enormous clue in the mystery of missing antimatter and proliferation of matter in cancer. The way they do that is to look first for a very rare form of beta decay, called **double beta decay.** That’s when **two neutrons in the nucleus of an atom simultaneously decay.** If neutrinos are their own antiparticle, an even rarer thing can occur called **HYBRID neutrinoless double beta decay** (the term: Robert Skopec). In this process, **the neutrinos are absorbed before they get outside of the nucleus.** In this case **no neutrinos are emitted.** The observation of a single, unambiguous neutrinoless double beta decay would show that **matter and antimatter neutrinos were the same.**
If indeed neutrinoless double beta decay exists, it’s very hard to detect and it’s important that scientists can discriminate between the many types of radioactive decay that mimic that of a neutrino. This requires the design and construction of very precise detectors. So that’s what the Majorana Demonstrator scientists achieved. Once and for all, it can answer the question of whether matter and antimatter neutrinos are HYBRID: the same or different. With that information in hand, it might be possible to understand why our Universe is made of matter leading to cancer too. (Lincoln, 2018)

3. HYBRID Majorana Fermion Change the World

Chinese scientists won a major victory, by proving that the Majorana fermion – a particle we’ve found tantalizing hints of for years – genuinely exists. This discovery has huge implications for quantum computing of cancer, and it might change the World.

A Majorana fermion is weird even by the standards of quantum physics. The Majorana fermion doesn’t have a charge, which allows the mystery of cancer to be HYBRID: matter and anti-matter at the same time! The fact that it doesn’t have a charge, and also happens to be the exact reverse of itself at the same time.

Quantum computers of cancer, are like a huge pile of dimmer switches. You can set these dimmers much, much faster than you can flip on this light switches, because the dimmers are all wired to each others, immediately as tumors. These dimmers, e. i. quantum bits, are what’s called entangled in cancer. If you change one quantum bit, the others it’s entangled with change with it, even if they’re a million miles away from each other.

That’s where Majorana fermions as metastasis come in due to their HYBRID: no-charge nature. (Seitz, 2018)

4. Results

The neurological basis of synesthesia could help explain one skill that many creative people share facility for using metaphor to make links between seemingly unrelated domains. Metaphor involves making links between seemingly unrelated conceptual realms, while this is not just a coincidence. Cancer Coincidences is at a deeper level a manifestation of HYBRID Quantum Entanglement Entropy. (Lin et al., 2014) Mutation of the angular gyrus make possible for synesthesia to provide excess communication among different brain maps. Involved in cross-modal synthesis the brain regions where information from touch, hearing and vision flow together are enabling the construction of high-level perceptions. The angular gyrus is disproportionately larger in humans than in apes and monkeys – evolved originally for cross-modal associations. Probably later became co-opted for more abstract functions such as metaphors. (Ramachandran and Hubbard, 2001)

The common abstract property is extracted somewhere in the vicinity of the TPO, probably in the angular gyrus. It is extracting the abstraction of the common denominator (“ratio”) from a set of strikingly dissimilar entities. When the ability to engage in cross-modal proliferation of metastasis emerged, it is opening the way for more complex types of abstraction – e. i. for geniality of thinking. (Skopec II., 2018)

4.1 HYBRID Fourth Dimension of Alternate Reality

We can try to picture a fourth dimension. Veer left for a second dimension, and then jump up for a third dimension. Then dive into a fourth dimension, in a direction we don’t have a word for because our minds can’t grasp even the idea of it. That’s a fourth dimension of space, about which two new studies yield some clues.

Scientific experiments can’t grasp a fourth dimension any better than we can. But if scientists can design them very carefully, their studies can produce shadows of a sort, which suggest a fourth dimension really is there lurking just beyond our grasp. Two such physics experiments have done just that, according to two papers published in the journal Nature. The research was conducted mostly by independent teams tackling similar big questions with very different little questions, although one co-author was involved on both projects.

Researchers used two different approaches to dance around the idea of a fourth dimension. They looked for a specific type of theorized fingerprint that is two-dimensional and therefore within our capabilities instead, as Gismodo has reported. In both cases, the experiments demonstrated phenomena that actually require just two dimensions, nice and mundane.

The tools required to get those phenomena to manifest were anything but mundane. One experiment relied on lasers to trap individual atoms of a highly reactive element called rubidium in a square, like a cat carefully sitting between taped lines. The other experiment used a box and seeing how the effects rippled throughout the box. Studies let scientists explore fourth dimension theories in new ways. The physicists on both these projects aren’t just looking for a nice brainteaser, of course. They want to stretch our knowledge and technology as far as
possible. Even if we can’t actually experience a fourth dimension ourselves, they think reaching for the fringes of it could offer valuable lessons that we can implement right here in the 3-D world we live in.

Maybe we can come up with new physics in the higher dimension and then design devices that take advantage of the higher-dimensional HYBRID physics in lower dimensions. (Rechtsman et al., 2018)

4.2 HYBRID Nonlinear Deviation Term

Neurobiological correlates of value have been described in orbitofrontal (conscience), cingulated cortex (critical intellectuals) and the basal ganglia, areas of the brain traditionally associated with reward-seeking behavior. Some neurons in orbitofrontal cortex represent value independently from evidence, choice and action. Anterior cingulate cortex is thought to represent negative (critical, non-linear) value. (Gold & Shadlen, 2007)

There is much evidence that a number of brain regions are sensitive to expected reward (or “utility”). The most well established are dopaminergic regions such as the striatum and midbrain structures. The common ratio pattern can be reconciled by the plausible assumption that people apply nonlinear decision weights \( \pi(p) \) to objective probabilities \( p \), so that the ratio \( \pi(0.02)/\pi(0.01) \) is much smaller than \( \pi(1)/\pi(0.5) \).

Neural responses to probabilities resembling the smoothly increasing function which typically fit behavior well. Paulus and Franck (2006) focused on between subjects measures and showed that activity in anterior cingulate correlated with degree of nonlinearity across subjects. We can make the assumption that neural activity is approximately a linear function of the behaviorally derived utility function. The GLM model separates the weighting function into two components: (1) component that is linear in \( p \) and (2) the component that is the nonlinear deviation term (NDT) \( \Delta(p, \alpha) = \pi(p, \alpha) - p \).

Specifically, we are looking for a prospect-theoretic expected value function that is nonlinear in \( p \); that is \( \pi(p, \alpha)u(x) = p \cdot u(x) + \Delta(p, \alpha) \cdot u(x) \). We assume the function \( u(x) \) is power function \( x^\mu \), where the value of \( p \) is taken from the individual behavioral estimate, and \( \Delta(p, \alpha) = \pi(p, \alpha) - p \), where the mean group \( \alpha \approx 0.771 \) is used.

If the expected utility (EU) null hypothesis is an accurate approximation of valuation of risky choices, there should be no reward-related brain regions that respond to the deviation term \( \Delta(p, \alpha) \cdot u(x) \). If the nonlinear weighting hypothesis is an accurate approximation, there should be reward-related brain regions that respond equally strongly to the linear component \( p \cdot u(x) \) and to the nonlinear component \( \Delta(p, \alpha) \cdot u(x) \).

We can test whether cross-subject variation in the inflection of nonlinear weighting inferred from choices is consistent with cross-subject differences in neural activity caused by cancer. More highly nonlinear functions will be approximated by a combination of the linear term \( p \) and the nonlinear term \( \Delta(p, \alpha) = \pi(p, \alpha) - p \) that puts more weight on the nonlinear term. A linear-weighting subject, will put no weight on nonlinear deviation \( \Delta(p, \alpha) = \pi(p, \alpha) - p \) of tumors.

Denote the true weighting function for subject \( i \) by \( \pi(p, \alpha) \), and the deviation from linear weighting by \( \Delta(p, \alpha) = \pi(p, \alpha) - p \). A brain region that represents \( \pi(p, \alpha) \) will be significantly correlated with both \( \Delta(p, \alpha) \) and \( p \).

That is, the linear term \( p \) and nonlinear deviation term with a higher weight on the nonlinear deviation term. (Hsu et al., 2009) Brain regions that are governing the cancer significantly correlated with the nonlinear term include the anterior cingulated cortex (ACC), the striatum, motor cortex, and cerebellum. Our intuition is that brain activity during valuation of risks is more likely to correspond to cognitive components of prospect-masking in cancer, than to EU, and it will be easier to construct an adaptationist account of how evolution would have shaped brains to follow prospect-masking in cancer rather than EU. The prospect-masking follows from psychophysics of proliferation, while EU from normative logic. (Hsu et al., 2009)

The increased specialization required today for professional credentials makes the broad thinking of that characterizes geniuses harder to develop. I agree that the ritual culture of academia may also hamper genius. As philosopher of science Thomas Kuhn has pointed out, highly creative work (without precedent) does not fit existing formalistic academic paradigms tend to be dismissed the counter-selection leading to cancer. (Skpec
III., 2015) Many great scientists have related how their most original ideas were repeatedly rejected by their peers and caused cancer.

4.3 Dichotomous Correlations of Cancer HYBRID Adaptation

One prevalent description of translational medicine, first introduced by the Institute of Medicine’s Clinical Research Roundtable, highlights two roadblocks (i.e., distinct areas in need of improvement): the first translational block (T1) prevents basic research findings from being tested in a clinical setting; the second translational block (T2) prevents proven interventions from becoming standard practice.

An important role in the processes of adaptation and masking in humans is playing also the immune system. The innate immune system functions as an interpreter of tissue damage and provides a first line of defense, also translates the information to other repair and defense systems in the body by stimulating angiogenesis, wound repair, and activating adaptive immunity. It is appropriate to consider autophagy a means for programmed cell survival balancing and counter-regulating apoptosis. Autophagy seems to have a dichotomous role in tumorigenesis and tumor progression.

Two other attributes play a similarly paradox role. The first involves major reprogramming of cellular energy metabolism in order to support continuous cell growth and proliferation replacing the metabolic program that operates in most normal tissues. The second involves active evasion by cancer cells from attack and elimination by immune cells. This capability highlights the dichotomous correlations of an immune system that both antagonizes and enhances tumor development and progression.

Evidence began to accumulate in the late 1990s confirming that the infiltration of neoplastic tissues by cells of the immune system serves counter-intuitively to promote tumor progression. (Skopec III., 2015)

4.4 The Bipolar Nature of Cancer: HYBRID, Two Faced New Main Law of Nature

The quantum entanglement is a basis of twofaced reality in which we are living our lives. From this reality are outgoing also the science and healthcare too. Although metastasis is important for systemic correlations expansion (as in tumors), it is a highly dichotomous process, with millions of cells being required to disseminate to allow for the selection of cells-correlates aggressive enough to survive the metastatic cascade. To quantify the dynamics of metastasis of correlations development, we need look at the coincidences of metastases in terms of co-occurrence at every point of time. To quantify co-occurrence we can use the \( \varphi \)-correlation between dichotomous variables defined as:

\[
\frac{N_X(t)C_\varphi(t) - m_i(t)m_j(t)}{\sqrt{m_i(t)m_j(t)[N_X(t) - m_i(t)][N_X(t) - m_j(t)]}}
\]

where \( C_\varphi(t) \) is the number of co-occurrence at time \( t \).

Than i and j represent particular site of metastasis, \( X \) represents the primary correlations type. The pair-wise correlations (coincidences) between metastasis network links for every primary correlations types and lead to the correlation coefficient matrix.

The dichotomous correlations of the adaptation may be caused also by the Quantum Entanglement Relative Entropy as a measure of distinguishability between two quantum states in the same Hilbert space. The relative entropy of two density matrices \( p_0 \) and \( p_1 \) is defined as \( S(p_1|p_0) = \text{tr}(p_1 \log p_1) - \text{tr}(p_1 \log p_0) \). When \( p_0 \) and \( p_1 \) are reduced density matrices on a spatial domain \( D \) for two states of a quantum field theory (QFT), implies that \( S(p_1|p_0) \) increases with the size of \( D \). Then \( \Delta S_{\text{EE}} = -\text{tr}(p_1 \log p_1) + \text{tr}(p_0 \log p_0) \) is the change in entanglement entropy across \( D \) as one goes between the states.

When the states under comparison are close, the positivity is saturated to leading order: \( S(p_1|p_0) = \Delta(H_{\text{mix}}) - \Delta S_{\text{EE}} = 0 \). (Skopec II., 2018)

The problem of conventional adaptation may be given by a definition of static, deterministic world. The proliferative correlations lead to the resonances between the degrees of freedom. When we increase the value of energy, we increase the regions where randomness prevails. For some critical value of energy, chaos appears: over time we observe the exponential divergence of neighboring trajectories. For fully developed chaos, the cloud of points generated by a trajectory leads to diffusion. (Prigogine, 1997) Here we must as first formulate a new Main Natural Law: the HYBRID Quantum Entanglement Entropy (HQEE). (Skopec III.,
2015) Through above resonances the QEE is causing a metastasis of correlations, antagonistically intertwining (coincidences) all types of potentially conflicting interests in cancer.

4.5 Secret Particles in Quantum Theory

Physicists have done the seemingly impossible: found a way to track mysterious quantum particles even when those particles aren’t being observed. In classical physics, an object occupies only one state of being at a time, something could be either alive or dead, but not both simultaneously. But quantum physics, which seeks to explain how life works at the subatomic level, isn’t so intuitive. Quantum physics differs from classical physics in that under quantum theory, objects can exist as both waves and particles, occupying both states at the same time. They only exist as either one or the other after they’ve been measured.

Researchers from the University of Cambridge have shown that the movements of those particles actually can be tracked without measuring them first – by observing the way the particles interact with their surrounding environments. A paper describing the work was published in the scientific journal Physics Review A.

Think of Schrödinger’s cat, the standard paradox for illustrating this particular aspect of quantum theory. Premise of Schrédinger’s cat, commonly referred to as the wave function, has been used more as a mathematical tool than a representation of actual quantum particles, first author David Arvidsson-Shukur, a Ph.D. student at Cambridge’s Cavendish Laboratory, said in the statement. That’s why they took on the challenge of creating a way to track the secret movements of quantum particles.

When any particle interacts with its environment, it leaves a tag. Those tags result in information being encoded into particles. D. Arvidsson-Shukur and his colleagues theorized a way that physicists could map how quantum particles tag their environments without their having to look directly at the particles. Researchers are able to explore the forbidden domain of quantum mechanics: pinning down the path of quantum particles when no one is observing them.

Another hypothetical scenario used by some scientists to illustrate quantum particles is called counterfactual communication. In counterfactual communication, information can be shared between two people, without any particles actually travelling in the space between them. This concept is akin to telepathy. It’s called counterfactual because the traditional facts would hold that particles would have to move between Alice and Bob in order for a message from one to the other.

To measure this phenomenon of counterfactual communication, we need a way to pin down where the particles between Alice and Bob are when we’re not looking. Above tagging method can do just this. The researchers believe their new technique could help quantum physicist follow the movements of particles they’re experimenting on throughout the whole process – even if they don’t actually measure them until the very end. (Medrano, 2017)

4.6 HYBRID Quantum Computing Apocalypse

In the ancient world, they used cubits as an important data unit, but the new data unit of the future is the qubit – the quantum bits that will change computing. Quantum bits are the basic units of information in quantum computing, a new type of computer in which particles like electrons or photons can be utilized to process information with both sides (polarizations) acting as a positive or negative, alternatively or at the same time.

According to experts, quantum computers will be able to create breakthroughs in many of the most complicated data processing problems, leading to the development of new medicines, building molecular structures and doing analysis going far beyond the capabilities of today’s binary computers.

The elements of quantum computing have been around for decades, but it’s only in the past few years that a commercial computer that could be called quantum has been built by a company called D-Wave. Announced in January 2018, the D-Wave 2000Q can solve larger problems than was previously possible, with faster performance, providing a big step toward production of applications in optimization, cybersecurity, machine learning and sampling.

IBM announced that it had gone even further – and that it expected and it would be able to commercialize quantum computing with a 50-qubit processor prototype, as well as provide online access to 20-qubit processors. That was followed by Microsoft announcement of a new quantum computing programming language and stable topological qubit technology that can be used to scale up the number of qubits.

Taking advantage of the physical spin of quantum elements, a quantum computer will be able to process simultaneously the same data in different ways (HYBRID), enabling it to make projections and analyses much more quickly and efficiently than now is possible. There are significant physical issues that must be worked out, such as the fact that quantum computers can only operate at cryogenic temperatures (at 250 times
colder than deep space) – but Intel, working with Netherlands firm QuTech, is convinced that it is just a matter of time before the full power of quantum computing is unleashed.

Their quantum research has progressed to the point where partner QuTech is simulating quantum algorithm workloads, and Intel is fabricating new qubit test chips on a regular basis in their leading-edge manufacturing facilities. Intel Labs expertise in fabrication, control electronics and architecture sets us apart and will serve us well as venture into new computing paradigms, from neuromorphic to quantum computing.

The difficulty in achieving a cold enough environment for a quantum computer to operate is the main reason they are still experimental, and can only process a few qubits at a time – but the system is so powerful that even these early quantum computers are shaking up the world of data processing. On the one hand, quantum computers are going to be a boon for cybersecurity, capable of processing algorithms at a speed unapproachable by any other system.

By looking at problems from all directions – simultaneously (HYBRID) – a quantum computer could discover anomalies that no other system would notice, and project to thousands of scenarios where an anomaly could turn into a security risk. Like with a top-performing supercomputer programmed to play chess, a quantum-based cybersecurity system could see the moves an anomaly could make later on – and quash it on the spot.

The National security Agency, too, has sounded the alarm on the risks to cybersecurity in the quantum computing age. Quantum computing will definitely be applied anywhere where we’re using machine learning, cloud computing, data analysis. In security that means intrusion detection, looking for patterns in the data, and more sophisticated forms of parallel (HYBRID) computing.

But the computing power that gives cyber-defenders super-tools to detect attacks can be misused as well. Scientists at MIT and the University of Innsbruck were able to build a quantum computer with just five qubits, demonstrating the ability of future quantum computers to break the RSA encryption scheme.

That ability to process the zeros and ones at the same time means that no formula based on a mathematical scheme is safe. The MIT/Innsbruck team is not the only one to have developed cybersecurity-breaking schemes, even on these early machines, the problem is significant enough that representatives of NIST, Toshiba, Amazon, Cisco, Microsoft, Intel and some of the top academics in the cybersecurity and mathematics worlds met in Toronto for the yearly Workshop on Quantum-Safe Cryptography last year.

The NSA’s Commercial National Security Algorithm Suite and Quantum Computing FAQ says that many experts predict a quantum computer capable of effectively breaking public key cryptography within a short time.

According to many experts, the NSA is far too conservative in its prediction, many experts believe that the timeline is more like a decade and a half, while others believe that it could happen even sooner. And given the leaps of progress that are being made on almost a daily process, a commercially viable quantum computer offering cloud services could happen even more quickly, the D-Wave 2000Q is called that because it can process 2,000 qubits. That kind of power in the hands of hackers makes possible all sorts of scams that don’t even exist yet.

Forward-looking hackers could begin storing encrypted information now, awaiting the day that fast, cryptography-breaking quantum computing-based algorithms are developed. It’s certain that the threats to privacy and information security will only multiply in the coming decades. In fact, why wait? Hackers are very well-funded today, and it certainly wouldn’t be beyond their financial abilities to buy a quantum computer and begin selling encryption-busting services right now. It’s likely that not all the cryptography-breaking algorithms will work on all data, at least for now. This is a threat-in-formation – but chances are that at least some of them will, cyber-criminals could utilize the cryptography-breaking capabilities of quantum computers, and perhaps sell those services to hackers via the Dark Web.

The solution lies in the development of quantum-safe cryptography, consisting of information theoretically secure schemes, hash-based cryptography, code-based cryptography and exotic-sounding technologies like lattice-based cryptography, multivariate cryptography (like the Unbalanced Oil and Vinegar scheme), and even supersingular elliptic curve isogeny cryptography.

These, and other post-quantum cryptography schemes, will have to involve algorithms that are resistant to cryptographic attacks from both (HYBRID) classical and quantum computers, according to the NSA. It’s certain that the threats to privacy and information security will only multiply in the coming decades and that data encryption will proceed with new technological advances. (Dolev, 2018)
Acknowledgments

The author gratefully acknowledge the assistance of Dr. Marta Ballova, Ing. Konrad Balla, Livuska Ballova and Ing. Jozef Balla.

References

Bartels M: Newsweek, Jan. 5, 2018
Dolev Sch (2018) The quantum computing apoclypse is imminent. TechCrunch, 6.1.2018
Mikael Rechtsman et al., (2018), Penn State Univesity, Nature

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.
This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/)