Crypto News

Compiled by
Dhananjoy Dey
IIIT Lucknow
Chak Ganjaria, C. G. City
Lucknow – 226 002
email: dhananjoy.dey@gov.in

September 1, 2020

Contents

August 2020

31 Aug 2020

1 How Cryptography Lets Down Marginalized Communities

by Lily Hay Newman

https://www.wired.com/story/seny-kamara-crypto-encryption-underserved-communities/

ONE OF THE perennial highlights of the International Association for Cryptologic Research's Crypto conference is the "invited talk." For an hour each year, a prominent scholar shares a big idea or new perspective on the protocols, algorithms, and math problems that underlie cutting-edge encryption. It's usually a deeply technical bacchanal, but this year was not. Prolific academic cryptographer Seny Kamara of Brown University had something other than formulas and theorems on his mind.

"So an actual question then is OK, well, what am I doing here, right?" Kamara asked the livestream attendees. "Why am I giving a talk at Crypto if I'm not talking about technical things? And, you know, basically I'm here because Ahmaud Arbery was killed in February, because Breonna Taylor was killed by a police officer in March, and because George Floyd was also killed by police officers in May."

The talk, dubbed Crypto for the People and given on August 19, examined the question of who really benefits from encryption technologies and advances in cryptographic research. It sounded a call to reexamine research priorities that today largely serve the interests of governments and corporations instead of marginalized people, be they racial minorities, immigrants, women, the LGBTQ community, or others. As an immigrant and Black American – and one of the few Black academic cryptographers in the world – Kamara pointed out that even the open source community and movements like the cypherpunks largely don't directly work to address these needs. They are focused on taking power from corporations and developing technologies to defend people from mass government surveillance and digital intrusion, but generally not on developing encryption technologies and new areas of abstract theory that are specifically motivated by the needs of underserved communities.

"As long as I've been studying and working in cryptography and computer science, about 20 years now, it was always very clear to me that my own work and other people's work was disconnected from my life experiences," Kamara tells WIRED. "I believed it could have an impact on people's privacy as a whole, but I didn't think I would have cared about any of it when I was 13 or 15 and growing up in New York City. And that disconnect always bothered me."

So much of cryptographic research is abstract and mathematical – divorced from real-world conditions – that it can be easy to simply let all lines of inquiry exist only in that theoretical space. And Kamara argues that even when encryption technologies are brought to underserved communities, they arrive retrofitted from other research projects, rather than conceived based on the needs of the vulnerable and the specific threats they face.

"As academics working on policy questions, we motivate our work in grant applications and so on by arguing that it benefits the people in some way," says Abdoulaye Ndiaye, a macroeconomics researcher at New York University who discovered Kamara's Crypto talk on Twitter. "However, the consumers of our research are other academics, government institutions, and, in some fields, businesses. There is this underlying assumption that these entities will implement the research and it will trickle down to the underserved people. Dr. Kamara highlighted that in cryptography the incentives of the government and the business are not necessarily aligned with underserved people, the missing link in this trickle down."

Encryption technologies do provide protection to vulnerable groups around the world like political dissidents, activists, and journalists. Kamara's talk made the case, though, that purpose-built cryptography could accomplish so much more.

In his own research at Brown, for example, Kamara and his colleagues have done work motivated by law enforcement databases in the United States that track alleged criminals like possible gang members. In a 2015 audit of a California state platform called CalGang, for example, 42 people entered in the database were under the age of 1 year old. In a sample of 100 entries from the database, 13 of the people represented should not have been in the database at all, and 131 of the 563 evidence points used against the 100 people were not supported.

So Kamara has worked on developing secure database schemes in which data can be audited and checked privately but transparently, that does not allow data to be exported or duplicated, and that deletes entries automatically after a given amount of time without special authorization from an authority like a judge.

"I think there is an intersection between traditional cryptography and privacy and what I was calling 'crypto for the people,'" Kamara says. "There is research and there are tools that can be beneficial to large subsets of people, as in the encrypted messaging app Signal. But there are also problems and adversarial models that are unique to marginalized groups, and those problems are not being investigated. For example, not everyone ends up in a gang database, and certainly very few cryptographers or academic computer science researchers end up in gang databases."

Kamara also advocated using the flexibility and security of tenured professorships as an opportunity to push the envelope of what cryptographic research can be – including in the case of his own talk. "I went into it thinking, 'I'm glad I have tenure, because this is going to cost me,'" he says. But Kamara says the response has been very positive so far. "I'm sure there are many others who disagree and didn't like the talk, but so far they haven't reached out to let me know," Kamara says.

The long-standing question of morality in cryptography rarely makes it to the foreground, even within the academic community itself. The discourse flared up in the wake of Edward Snowden's 2013 revelations about mass digital surveillance by the National Security Agency, particularly after a seminal 2015 paper by UC Davis cryptographer Phillip Rogaway, which made the case that cryptography is "an inherently political tool" with "an intrinsically moral dimension."

"I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work," Rogaway wrote.

Five years later, he says he doesn't see many changes in the research most cryptographers are doing or the topics they are discussing at conferences. But he adds that he was impressed with Kamara's talk and the steps it took to move the discourse forward. The essay Rogaway wrote in 2015, he says, would now include not just a discussion of the ethical need to defend the masses against mass surveillance, but an entreaty that the academic community focus more of its work on serving marginalized groups.

"We don't work in a vacuum and we're not pure mathematicians," Rogaway told WIRED. "As much as certain cryptographers would like to see themselves as doing pure mathematics on some kind of quest of discovery, that's not an apt description of where we sit. The field does have these very strong political connections and connections to power. And if we just say, 'Oh, that's not my domain,' that in itself is a really politically situated, ahistorical view and ultimately quite elitist."

Today, partly because of rapidly expanding anti-abuse work on social networks and communication platforms, the idea of an ethical imperative in privacy technologies has become more mainstream. But much of the actual work in cryptography remains fundamentally abstract. The practical applications that

do exist often originated with a narrow field of view.

"Building the same stuff you always did but claiming that it's for people in marginalized communities is not the same thing as human-centric threat modeling," wrote Lea Kissner, a cryptographer and security engineer focused on anti-abuse and privacy, in a series of tweets about Kamara's talk last week.

The type of tailored, threat-specific research Kamara described requires intimate knowledge of the actual, nuanced needs of a marginalized group. Kamara emphasized in his talk that the cryptography community needs to be much more inclusive and representative if it wants to help the vulnerable. And researchers need to seek firsthand expertise to gain a deeper understanding case by case.

"I think the only reason we have a hard time imagining what this looks like is because, effectively, we've been trained for 40 years to do corporate research. So we lack the imagination, skills, and knowledge to do research 'for the people,'" Kamara says. "But diversity is crucial for this."

Following the shootings of Breonna Taylor, George Floyd, and Jacob Blake, Kamara says fellow cryptographers and other computer scientists have reached out to him to talk about systemic changes that could be aided by technical solutions to reduce police brutality. Kamara says he welcomes these discussions, "but most of those people have never been attacked by the police. They don't understand the psychological pressure you're under and the confusion you're experiencing when five cops are running at you. These kinds of details matter."

2 Is Critical Infrastructure Ready for Quantum?

by Scott Totzke

https://www.infosecurity-magazine.com/opinions/critical-infrastructure-quantum/

There is no doubt that quantum technology will deliver a magnitude of benefits, solving very specific problems that even the fastest supercomputers cannot solve. Consider the impact quantum applications will have on satellite communications, autonomous driving vehicles, and molecular mapping capabilities.

Yet, many exciting innovations that quantum technology promises may never be realized if we don't take a proactive posture first to protect our data and systems, and prepare for the future. Collectively, we want to realize all of the benefits of quantum without compromising security.

The fact is, quantum computers will be able to break the cryptography underlying public key infrastructure (PKI), posing an unprecedented problem for encryption and authentication that enterprises put their trust in today. The services and infrastructure that we depend on most for our security, governance, public health, and safety are already at risk for cyber-attacks. That risk will increase exponentially with the advent of quantum computers.

The NIST National Cybersecurity Center of Excellence (NCCoE) has already put in place several practices "to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks," according to its latest update.

Cryptography is the foundation of digital trust

Core industries including energy, automotive, and Internet of Things manufacturing, depend on a trusted, cryptographic architecture for security at multiple levels: a threat to cryptography is a serious threat to digital trust.

Broken cryptography can result in unauthorized access to sensitive information and lack of control over connected devices. Consider the impact on a nuclear plant, an autonomous vehicle, or an embedded pacemaker.

Quantum technology will have a tremendous effect on organizations' trust infrastructure. Imagine a pyramid, with cryptography at every layer, the glue holding everything together. If one layer erodes, it could wreak havoc on our trust infrastructures in every industry and sector with catastrophic results.

The energy sector, especially, has already been vulnerable to cyber-attacks. Today's exploits generally happen in the top layers: compromised user credentials, admin system misconfiguration. With quantum computing, the most trusted elements – identity infrastructure, platform, architecture – become easier to attack, leading to more severe breaches.

Planes, trains, and automobiles ... and energy grids

Airplanes, automobiles, satellites, energy grids. These durable, critical devices are highly vulnerable to attack, as these connected devices have long in-field lives requiring their software/firmware signing trust anchors to be updated. Imagine a state-sponsored hack intercepting and then forging software updates for a satellite.

Let's take a look at the automotive industry. It is currently undergoing an electrification process. In a few years, every new vehicle sold will have some degree of autonomy built in. Quantum technology can help here a great deal; for example, with designing more efficient and safe batteries.

At the same time, these vehicles will increasingly rely on software that will need to be updated periodically to fix issues or add new functionality. Today, these updates are mostly performed manually when physically servicing the vehicle.

The next big OS war is in your dashboard, says a Wired article. Consider this. New cars roll off the assembly line with 100 million lines of code; this number will easily double with autonomous features. It will become essential to ensure that over-the-air (OTA) updates are authenticated and secure.

In order to perform these updates, automobile manufacturers need to build in and deploy quantum-safe, updatable components. Quantum-safe mechanisms will verify that the updates are not forged and are coming from the original equipment manufacturers.

Imagine the billions of dollars of cost savings if car manufacturers could update a component and handle cryptographic changes and eliminate recalls for electric issues – without requiring in-person maintenance and updating.

Recalls are common; recent electrical issue recalls: Kia recalled more than 200,000 vehicles this year; Fiat Chrysler Automobiles recalled more than 182,000 vehicles in 2019; and Volkswagen recalled 679,000 cars in 2018. Imagine the improved user experience these updates will offer: increased well-being and safety and less hassle of not having to schedule an appointment.

In the energy sector, we have seen power grids become the target for nation-orchestrated cyber-attacks, where equipment has been in place for decades. "The power sector has become a prime target for cyber criminals in the last decade, with cyberattacks surging by 380% between 2014 and 2015," according to an article in Power Technology. EV charging stations, the intersection of two critical infrastructures – transportation and energy – could be exploited to harm other sections, warns E&E News.

A system that is vulnerable now will be exponentially more at risk when quantum technologies arrive. What can organizations do now to strengthen and future-proof their cryptographic infrastructures?

Organizations with mission-critical security requirements can strengthen and start future-proofing their cryptographic infrastructures today. They can start preparing for quantum computing now by making their systems crypto agile.

A good first step is to inventory systems and algorithms. A few questions to determine quantum preparedness urgency:

- How many years does the device need to be secured for?
- How long does the information need to remain confidential?

If the answer to either question is more than seven years – jet engines, pacemakers, cars – start preparing today. Bridging the gap between current and quantum-safe security will require a new approach. Many organizations are looking to adopting a crypto agile posture without affecting existing systems, adherence to standards, and end users.

The ISARA Catalyst Agile Digital Certificate Technology is an example of a crypto agility methodology for creating an enhanced X.509 digital certificate that simultaneously contains two sets of cryptographic subject public keys and issuer signatures. Enhanced X.509 certificates are compliant with industry standards and, if incorporated, will enable organizations to meet compliance. This allows organizations to perform a gradual migration by upgrading their most critical, at-risk assets in phases and with full backwards compatibility.

NIST urges, "It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks."

Currently, cybersecurity threats are like plugging a kitchen sieve. When quantum comes, the threats will be like plugging the Hoover Dam. Unless organizations take a proactive crypto agile posture today.

3 New theory hints at more efficient way to develop quantum algorithms

by Kayla Wiles

https://phys-org.cdn.ampproject.org/c/s/phys.org/news/2020-08-theory-hints-efficient-quantum-algorithms.amp

In 2019, Google claimed it was the first to demonstrate a quantum computer performing a calculation beyond the abilities of today's most powerful supercomputers.

But most of the time, creating a quantum algorithm that stands a chance at beating a classical computer is an accidental process, Purdue University scientists say. To bring more guidance to this process and make it less arbitrary, these scientists developed a new theory that may eventually lead to more systematic design of quantum algorithms.

The new theory, described in a paper published in the journal Advanced Quantum Technologies, is the first known attempt to determine which quantum states can be created and processed with an acceptable number of quantum gates to outperform a classical algorithm.

Physicists refer to this concept of having the right number of gates to control each state as 'complexity.' Since the complexity of a quantum algorithm is closely related to the complexity of quantum states

involved in the algorithm, the theory could therefore bring order to the search for quantum algorithms by characterizing which quantum states meet that complexity criteria.

An algorithm is a sequence of steps to perform a calculation. The algorithm is usually implemented on a circuit.

In classical computers, circuits have gates that switch bits to either a 0 or 1 state. A quantum computer instead relies on computational units called "qubits" that store 0 and 1 states simultaneously in superposition, allowing more information to be processed.

What would make a quantum computer faster than a classical computer is simpler information processing, characterized by the enormous reduction in the number of quantum gates in a quantum circuit compared with a classical circuit.

In classical computers the number of gates in circuits increases exponentially with respect to the size of the problem of interest. This exponential model grows so astonishingly fast that it becomes physically impossible to handle for even a moderately sized problem of interest.

"For example, even a small protein molecule may contain hundreds of electrons. If each electron can only take two forms, then to simulate 300 electrons would require 2300 classical states, which is more than the number of all the atoms in the universe," said Sabre Kais, a professor in Purdue's Department of Chemistry and member of the Purdue Quantum Science and Engineering Institute.

For quantum computers, there is a way for quantum gates to scale up "polynomially" – rather than just exponentially like a classical computer – with the size of the problem (like the number of electrons in the last example). "Polynomial" means that there would be drastically fewer steps (gates) needed to process the same amount of information, making a quantum algorithm superior to a classical algorithm.

Researchers so far haven't had a good way to identify which quantum states could satisfy this condition of polynomial complexity.

"There is a very large search space for finding the states and sequence of gates that match up in complexity to create a useful quantum algorithm capable of performing calculations faster than a classical algorithm," said Kais, whose research group is developing quantum algorithms and quantum machine learning methods.

Kais and Zixuan Hu, a Purdue postdoctoral associate, used the new theory to identify a large group of quantum states with polynomial complexity. They also showed that these states may share a coefficient feature that could be used to better identify them when designing a quantum algorithm.

"Given any quantum state, we are now able to design an efficient coefficient sampling procedure to determine if it belongs to the class or not," Hu said.

4 Quantum Innovations Achieved Using Alkaline-Earth Atoms

by Caltech

https://scienceblog.com/518215/quantum-innovations-achieved-using-alkaline-earth-atoms/

In the quest to develop quantum computers, physicists have taken several different paths. For instance, Google recently reported that their prototype quantum computer might have made a specific calculation faster than a classical computer. Those efforts relied on a strategy that involves superconducting materials,

which are materials that, when chilled to ultracold temperatures, conduct electricity with zero resistance. Other quantum computing strategies involve arrays of charged or neutral atoms.

Now, a team of quantum physicists at Caltech has made strides in work that uses a more complex class of neutral atoms called the alkaline-earth atoms, which reside in the second column of the periodic table. These atoms, which include magnesium, calcium, and strontium, have two electrons in their outer regions, or shells. Previously, researchers who experimented with neutral atoms had focused on elements located in the first column of the periodic table, which have just one electron in their outer shells.

In a paper published in the journal Nature Physics, the researchers demonstrate that they can use individually controlled alkaline-earth atoms to achieve a hallmark of quantum computing: entanglement. This seemingly paradoxical phenomenon occurs when two atoms remain intimately connected even when separated by vast distances. Entanglement is essential to quantum computers because it enables the computers' internal "switches," known as qubits, to be correlated with each other and to encode an exponential amount of information.

"Essentially, we are breaking a two-qubit entanglement record for one of the three leading quantum science platforms: individual neutral atoms," says Manuel Endres, an assistant professor of physics and leader of the Caltech team. Endres is also a member of one of three new quantum research institutes established by the National Science Foundation's (NSF's) Quantum Leap Challenges Institutes program, and a member of one of five new Department of Energy quantum science centers.

"We are opening up a new tool box for quantum computers and other applications," says Ivaylo Madjarov, a Caltech graduate student and lead author of the new study. "With alkaline-earth atoms, we have more opportunities for manipulating systems and new opportunities for precise manipulation and readout of the system."

To achieve their goal, the researchers turned to optical tweezers, which are basically laser beams that can maneuver individual atoms. The team previously used the same technology to develop a new design for optical atomic clocks. In the new study, the tweezers were used to persuade two strontium atoms within an array of atoms to become entangled.

"We had previously demonstrated the first control of individual alkaline-earth atoms. In the present work, we have added a mechanism to generate entanglement between the atoms, based on highly excited Rydberg states, in which atoms separated by many microns feel large forces from each other," says Jacob Covey, a postdoctoral scholar at Caltech. "The unique properties of the alkaline-earth atoms offer new ways to improve and characterize the Rydberg-interaction mechanism."

What is more, the researchers were able to create the entangled state with a higher degree of accuracy than had been previously achieved through the use of neutral atoms, and with an accuracy on par with other quantum computing platforms.

In the future, the researchers hope to expand their ability to control individual qubits, and they plan to further investigate methods to entangle three or more atoms.

"The endgame is to reach a very high level of entanglement and programmability for many atoms in order to be able to perform calculations that are intractable by a classical computer," says Endres. "Our system is also suited to investigate how such many-atom entanglement could improve the stability of atomic clocks."

5 Quantum computers may be heading underground to shield from cosmic rays

https://physicsworld.com/a/quantum-computers-may-be-heading-underground-to-shield-from-cosmic-rays/

Such is their sensitivity to environmental noise, quantum computers might in future be shielded by thick layers of lead and even operated deep underground. So say physicists in the US, who have found that ionizing radiation significantly limits the coherence time of superconducting qubits. Indeed, they say that minimizing radiation effects will be crucial if general-purpose quantum computers are to be made using superconducting technology.

Quantum computers can perform certain calculations much more quickly than classical computers by storing and processing information using quantum bits (qubits). Superconducting circuits are among the leading types of qubit currently under development, generating superpositions of 0s and 1s from the ground and first excited states of an anharmonic oscillator formed from the combination of Josephson junctions and a capacitor. Although they need to be cooled down to very low temperatures, such qubits are solid state and therefore hold the promise of being relatively easy to manufacture and integrate.

Indeed, last year John Martinis and colleagues at Google used a processor comprising 53 superconducting qubits to execute a very specific algorithm more than a billion times faster than they say would be possible using one of the world's leading conventional supercomputers – although this billion-fold advantage has since been disputed.

Minimum coherence time

Superconducting qubits can currently retain their delicate quantum states – their "coherence" – for more than 100 μs. While this much better than the nanoseconds of two decades ago, coherence times will need to increase by several orders of magnitude before the qubits can be used in general-purpose fault-tolerant computers. These devices would rely on error correction and can only work efficiently if the error rates on individual qubits and gates are already below a certain threshold – implying a minimum coherence time.

Coherence is impeded by a wide range of noise sources. On the timescale of tens or hundreds of microseconds, material defects, magnetic moments and trapped charges, among others, tend to cause the biggest headaches. However, pushing coherence times up to and beyond a millisecond will require overcoming the problem of ionizing radiation. Beta particles, gamma rays and cosmic rays create electron-hole pairs within devices, which lead to cascades of energy and the breakup of the Cooper pairs responsible for the frictionless current in a superconductor.

Earlier this year, physicists in Germany and Italy reported that environmental radioactivity can impair the performance of superconducting resonators. The group, headed by Laura Cardani of the National Institute of Nuclear Physics in Rome and Ioan Pop of the Karlsruhe Institute of Technology, showed that cosmic rays and radioactive impurities can significantly increase the density of broken Cooper pairs, known as quasiparticles, within devices above ground. Conversely, by using a radio-pure set-up within Italy's Gran Sasso laboratory – located under 1400 m of rock – it was able to reduce the incidence of what are known as quasiparticle bursts by up to a factor of 50.

Ionizing effects

Now, William Oliver and colleagues at at the Massachusetts Institute of Technology (MIT) and the Pacific Northwest National Laboratory have taken this research a step forward by measuring and modelling the effect of ionizing radiation on superconducting qubits themselves. As they report in Nature, they did so using qubits made from aluminium mounted on a silicon substrate.

The team began by exposing two such qubits to a known source of ionizing radiation – a thin disc of copper-64 – and measured the rate at which qubits' decohere repeatedly over the course of several days (the copper having a half-life of just over 12 h). The idea was to establish how readily quasiparticles are generated in the qubits for a given flux of radiation.

The researchers then combined this information with measurements of the radiation present in the MIT lab, both from cosmic rays and naturally occurring radioactive isotopes – in the latter case, mainly from the lab's concrete walls. They calculate that the decohering effects of this radiation on the qubits would impose an upper limit to their coherence time of about 3-4 ms.

Lead bricks for shielding

To check this result with an independent experiment and establish how well such qubits might be shielded from ionizing radiation, the team surrounded seven such qubits (or rather the cryostat used to keep them cool) with 10 cm-thick lead bricks. This is the kind of shielding often used in neutrino and dark-matter experiments. By placing the shield on a scissor lift and periodically raising and lowering it, they were able to establish the effect of the external radiation thereby confirming the coherence limit of about 4 ms. They also found that the shield increased the coherence time by around 20%.

Given the existence of stronger sources of decoherence, Oliver and colleagues say that this shielding only raised the qubits' overall coherence time by about 0.2%. But they have no doubt that such noise-reduction measures will be needed if quantum computing is really to take off. "Reducing or mitigating the impact of ionizing radiation will be critical for realizing fault-tolerant superconducting quantum computers," they write.

One option, at least in the medium-term, would be operate devices underground. Oliver says that this would be a "good direction to go for verification and research". But he argues that for practical applications it would be better to design qubits that are less susceptible to quasiparticles. "That would allow us to keep superconducting quantum computers above ground," he says.

30 Aug 2020

6 Spain's timely edge for Quantum leadership

by Maria Luque

https://thequantumdaily.com/2020/08/30/spains-timely-edge-for-quantum-leadership/

Quantum communication, quantum sensing & metrology, quantum computation, Quantum Simulations & Basic Quantum Science development. Through short & long term applications of these Q-empowered fields, quantum technology is promised to act as an enabler for competitiveness in a wild, wild world. The deployment of such an adventure faces the usual caveats of faraonic missions / assignments: firstly, survive the swings of political winds and second, maintain momentum and relevance in a decades-long shot to keep the fuel (capital) the efforts (policy) and the talent (I+D) building the pyramid.

As industry alignment within the Quantum tech industry becomes a reality, the challenge of growing the Quantum muscle reveals itself as a needed collective effort. The people have to buy it, politicians have to see added-value for election campaigns in this adventure. The alignment in ethical & technical bottlenecks for Quantum deployment have to be agreed upon. The kid's gonna grow. It needs a consortium and ever-growing money flows. Will EU's approach to budgeting be up to the challenge? Or should nations themselves take the lead? Spain, with an awakening and proactive Quantum academia, spin-offs and high connectivity assets may have a shot at taking the lead.

> FOR EUROPE, IF A CONSORTIUM IS TO BE ESTABLISHED, IT MUST THINK OF ITS POWER AS STRONGLY-RELATED TO THE DEVELOPMENT OF QUANTUM LITERACY AND REGULATION WITHIN EU NATIONS. WHY?

Compared to US & China's outlay in Q-tech, the EU has accomplished a € 1 billion investment, to be used over 5 to 10 years through a now most-common instrument for overarching and potentially game-changer technologies: a FET Flagship. After the initial take off, Quantum Tech is contemplated to be included in the EU's Shaping Digital Europe Commission priority investments in 2022.

During 2020, reality checks and political winds have already arisen. The deployment of the Next Generation EU and the EU Recovery fund due to COVID19 has & will have some implications:

On the one side, it has already switched EU's funding priorities for the next year and a half: the program Shaping Digital Europe, expected to sustain the FET Flagship's initial Q-Tech ecosystem, has lowered its initial funding scheme by various millions for 2021 - 2024. Maybe this won't help to accomplish the 5 to 15 year quantum milestones & deliverables envisioned to grow the **Quantic EU**.

On the other side, a political turmoil is likely to stand in the way: as the EU Recovery fund incentive scheme returns power back to national governments, it'll be harder for the EU Commission to invest and dedicate faraonic resources in such an adventure.

It seems like EU Nations may need to take the lead when the moment comes, and develop their own quantum tech ecosystems. Helping the wider Flagship by envisioning their own priorities in research, applications & regulation, and positioning themselves to contribute to EU-wide beneficial quantum infrastructures, like the QCI.

> EU QUANTUM FUTURE'S SURVIVAL DEPENDS ON EU ¡¿ EU NATIONS ENTANGLEMENT. SPAIN MAY BE KEY IF WELL-PLAYED.

Spain: a timely edge for Quantum leadership

Strategically, Spain's particular conditions could earn it a leading place in the construction of the EU's Q-muscle. Let's see why.

Grand strategies for Quantum literacy depend more or less on this 5 focus areas:

- Enabling a strong foundation of capability with a skilled workforce (leading research ecosystem)
- Stimulating applications and market opportunity (business edge & market awareness)
- Creating the right social and regulatory context (networks, industry and academia alignment)

- Relying on acquired knowledge for past infrastructure faraonic adventures (experience on heavy asset deployment)
- International engagement within the Q-field (shared research, investment, industry initiatives)

The seeds for this Jackson five are already present.

In Spain, there's academia and there are small to medium size Quantum tech ventures and startups. The academia and the startups are heavily entrenched, being the latter mostly spin-offs of fine-tuned academic research programs in quantum computation and post-quantum encryption.

They are aware of their status as an ecosystem. Academia & incipient industry nodes network heavily and are aware of some of their most basic needs: the need for progress, the need to connect themselves to a wider Quantum International ecosystem (being active within the Q-tech Flagship, partnering with the likes of IBM & Microsoft), the need for alignment (producing ideas and solutions to technical & ethical bottlenecks) and the need to turn their research and public and private investments in marketable applications for survival.

An incipient, aware and more or less purpose-led Quantum ecosystem that shows some nodes asking for leadership in technical, networking and Q-application matters, and that is home to the first World Quantum Association.

An ecosystem that participates, through some of their brilliant startups and without government support in initiatives such as the Quantum Communication infrastructure (QCI), a promising adventure to withhold internal and digital security in the EU's future to come.

It's acquired knowledge on grand investments and infrastructure deployment are, too, paramount. Spain relies on international Telecom networks connecting the country with four continents – directly. It has positioned itself as a mooring point for alternate undersea cable routes within the Atlantic and heavy connection within the mediterranean. It lobbied to hold a vibrant industry for digital infrastructure processing and storing data, and is home to one of the EU pillars for supercomputation.

Seeds are in place. Now, where the funding and priorities are?

The "Quantum Spain" gets an "on hold" sign

This summer, Spain's Digital agenda has been served, on the rocks. In a nutshell, the strategic document "España digital 2025" paves the way for the digital transformation of the country for the next 5 years to come. Economically and socially.

The edges for the digital becoming of a country are many. Within the European & Atlantic environment, the bets rely on talent investment, education on digital literacy, eliminating bottlenecks for digital / online based businesses to thrive, data economy prioritization and heavy investment in technology enablers or drivers of change, such as IT infrastructure, blockchain or Quantum Tech. The ultimate enablers of healthy competitiveness, progress and safety for digital economies in decades to come.

Spain's agenda, on the other side, has chosen to omit investment strategies in these tech enablers, relegating Spain's Quantum momentum – and diminishing it's potential competitive edge – for the next five years. It may stay on hold for long.

Globally, Spain has no mirror where to look at. Heavy investment in tech enablers is not only a thing for big-game players like China and the US, nations that are paramount with the technique of flexible and

ever-growing investment in key capabilities. Europe's triad doesn't fall short for the next 5 years: with Germany 2.65 b, France 1.4 b and the UK with 1 b. The entire EU is investing itself through the Quantum FET Flagship – 1b – and more nuanced approaches like those of Netherlands 140 m, or infamous Smart Nation's Singapore with 25 m can be seen along the gallery.

Countries who want a shot at the future have strategically foresighted those technologies that would help them cross the leap once our internet and our computing capacities are drowned out, and our security compromised. Why not Spain? Let's see.

Spain's 2025 Digital Agenda is rather pragmatic. It takes up the baton from 2013's first agenda unfulfilled promises – relating digital transformation for SMEs and digital workforce upskilling – and focuses investment priorities and strategic alliances on its most deployed digital assets – connectivity infrastructure and 5G. No room for newbies.

Not a part of Spain's grand challenges for the next 5 years

The picture makes a lot of sense. Take it from here: Spain's grand challenge mimics the European Union's "A green, sustainable digital economy". And we've, Europeans, have successfully identified that the bottlenecks for a digital economy to spearhead its way into the future are four: to reach a common denominator of digitization in our public administrations, to enhance digitization in our economic fabric (SMEs), to foster digital literacy (upskilling & education) and to provide fuel via investing in IT and deep tech enablers for long-term competitiveness. Keeping up with its very strong "equality of access, equality of opportunity" principles.

Spain had a whole lot of overdue homework regarding the first three, so keeping up with the Kardashians consumes the already battered funding by more than half. In need to choose which deep tech / infrastructure asset to invest in, it decided to nurture what it already had deployed, high connectivity, data processing and storage, and 5G; bypassing the risks of faraonic investments in the likes of Blockchain and Quantum.

It's a smart choice that may give Spain a leading edge in the short term: in the end, the key for Next Generation's Digital Europe success involves building a sovereign and interoperable data cloud infrastructure. Spain can contribute positioning itself as the digital infrastructure node for Southern Europe. It pays off.

So there's the agenda: keeping up with the homework and giving a strategic shot to the resources we already count on.

Taking into account the bigger picture, the question here would be: should the Quantum industry remain idle for the next 5 years?

The answer is no: the longer the race, the harder the training.

The next step for the Spanish digital economy is thinking medium term: for that, Quantum is key.

The future of the EU and its position globally will be built upon the drivers of change and progress that we invest in, within this decade. Spain's shot at Quantum is real, and the path for a Quantum Spain can be cleared step to step.

These are times for the industry to align itself: their needs, their story, their contribution to the world and to the country, and start building the magic circle of momentum for a literacy, public and regulatory

support hard race. Events, dialogues, and the showing off roadshow can wait a little longer. Legitimacy – first, political, later, social – is better built upon an agreed story of success ... And of utility. Will it be up to the challenge?

28 Aug 2020

7 Intel's woes delays US' plan to make a supercomputer for exascale computing

by New York Times

https://economictimes.indiatimes.com/news/international/business/intels-woes-derails-us-plan-to-make-its-first-supercomputer-for-exascale-computing/articleshow/77791947.cms

When it selected Intel to help build a $500 million supercomputer last year, the Energy Department bet that computer chips made in the United States could help counter a technology challenge from China.

Officials at the department's Argonne National Laboratory predicted that the machine, called Aurora and scheduled to be installed at facilities near Chicago in 2021, would be the first U.S. system to reach a technical pinnacle known as exascale computing. Intel pledged to supply three kinds of chips for the system from its factories in Oregon, Arizona and New Mexico.

But a technology delay by the Silicon Valley giant has thrown a wrench into that plan, the latest sign of headwinds facing government and industry efforts to reverse America's dependence on foreign-made semiconductors. It was also an indication of the challenges ahead for U.S. hopes to regain a lead in critical semiconductor manufacturing technology.

Intel, which supplies electronic brains for most personal computers and web services, has long driven miniaturization advances that make electronic devices smaller, faster and cheaper. But Robert Swan, its chief executive, warned last month that the next production advance would be 12 months late and suggested that some chips for Aurora might be made outside Intel factories.

Intel's problems make it close to impossible that Aurora will be installed on schedule, researchers and analysts said. And shifting a key component to foreign factories would undermine company and government hopes of an all-American design.

8 BBVA and Multiverse benchmarked quantum solutions

https://www.swissquantumhub.com/bbva-and-multiverse-benchmarked-quantum-solutions/

BBVA is closely following through various lines of research aimed at exploring applications of quantum computing in the world of finance. As part of this work, and in collaboration with Spanish startup Multiverse, the joint research team has evaluated and benchmarked a number of quantum and traditional technologies to improve the process of dynamically optimizing investment portfolios with market data.

Multiverse is a Spanish tech startup that specializes in developing quantum algorithms for the international financial sector.

The results have allowed identifying unexplored methods to carry out these calculations that would allow maximizing the potential returns of investments. The purpose of this collaboration, still in an exploratory phase, has been to determine what weights in an investment portfolio containing certain assets yield higher returns.

They assessed and compared four quantum computing-based methods and two classical methods used in finance. Regarding quantum technologies, a method based on hybrid computing was run on the D-Wave Hybrid, as well as two other approaches built on the VQE (Variational Quantum Eigensolvers) algorithm, deployed in IBM's quantum computer Q System One. Finally, an attempt was made to solve the problem using a quantum-inspired algorithm based on Tensor Networks' platform.

The test carried out between BBVA and Multiverse places the bank at the cutting edge in the deployment of quantum technologies applied to quantitative finance. Since 2018, BBVA has collaborated in a number of quantum computing projects partnering with companies such as Fujitsu, Accenture, U.S. startup Zapata and Spain's Search Results, Spanish National Research Council.

26 Aug 2020

9 Chinese researchers expect quantum leap in computing, challenging Google's supremacy

https://www.globaltimes.cn/content/1198916.shtml

Chinese quantum computing researchers recently disclosed that a 60-qubit superconductivity quantum computing system with 99.5% fidelity could be achieved this year, and in 10 years, the system could evolve into a million-qubit level with a 99.8% fidelity, equivalent to, if not better than, its Google counterpart.

Zhu Xiaobo, a professor with the Shanghai-based Institute of Advanced Studies affiliated with University of Science and Technology of China, made the remarks on Tuesday, Shanghai news website Thepaper.cn reported.

The challenges of quantum computing development do not lie in the number of qubit, but it is the operation and control of each qubit that determines how advanced the system is, said Zhu, who is also in charge of the quantum computing work with the research team led by Chinese leading quantum physicist Pan Jianwei,.

US tech giant Google announced a breakthrough in October 2019 – using the company's state-of-the-art quantum computer, called Sycamore, Google has claimed "quantum supremacy" over the most powerful supercomputers in the world by solving problems considered virtually impossible for normal machines.

The Google quantum computer completed the complex computation in 200 seconds. That same calculation would take even the most powerful supercomputers approximately 10,000 years to finish, the team of researchers, led by John Martinis, an experimental physicist at the University of California, Santa Barbara, wrote in their study published in Nature magazine on October 23.

Zhu considered this breakthrough by Google a "really substantial one" in recent years, which is enabled by a 53-qubit superconductivity system with a 99.4% fidelity.

In quantum mechanics, notably in quantum information theory, fidelity is a measure of the "closeness" of two quantum states. It expresses the probability that one state will pass a test to identify as the other.

Zhu revealed that his team is close to achieving a 60-qubit quantum computer, seeking to catch up with and even surpass Google.

Zhu hopes that in 10 to 15 years, quantum computers can be used to solve real problems in the field of cryptology, rather than being used only to demonstrate their computing capabilities, which is the case for current models.

When the number of qubit reaches 100, and the computing system's fidelity reaches 99%, it can dwarf classical computers, he noted.

When a quantum computer is put into practical use, it will mainly play the role of a server. Users can upload their problems to the cloud and let the server work on them, Zhu said.

Pan's team declined to give further details of their studies when reached by the Global Times on Wednesday.

10 Scientists use reinforcement learning to train quantum algorithm

by Jared Sagoff

https://techxplore.com/news/2020-08-scientists-quantum-algorithm.html

Recent advancements in quantum computing have driven the scientific community's quest to solve a certain class of complex problems for which quantum computers would be better suited than traditional supercomputers. To improve the efficiency with which quantum computers can solve these problems, scientists are investigating the use of artificial intelligence approaches.

In a new study, scientists at the U.S. Department of Energy's (DOE) Argonne National Laboratory have developed a new algorithm based on reinforcement learning to find the optimal parameters for the **Quantum Approximate Optimization Algorithm** (QAOA), which allows a quantum computer to solve certain combinatorial problems such as those that arise in materials design, chemistry and wireless communications.

"Combinatorial optimization problems are those for which the solution space gets exponentially larger as you expand the number of decision variables," said Argonne computer scientist Prasanna Balaprakash. "In one traditional example, you can find the shortest route for a salesman who needs to visit a few cities once by enumerating all possible routes, but given a couple thousand cities, the number of possible routes far exceeds the number of stars in the universe; even the fastest supercomputers cannot find the shortest route in a reasonable time."

Developed recently, QAOA is considered as one of the leading candidates for demonstrating the advantage of quantum computers. QAOA is a hybrid quantum-classical algorithm that uses both classical and quantum computers for approximately solving combinatorial optimization problems.

The new algorithm developed at Argonne learns how to configure QAOA through a feedback mechanism. A particularity of the proposed algorithm is that it can be trained on smaller problem instances, and the trained model can adapt QAOA to larger problem instances. "It's a bit like having a self-driving car in traffic," Balaprakash said. "The algorithm can detect when it needs to make adjustments in the 'dials' it uses to do the computation."

The QAOA could have significant benefits for solving combinatorial problems that arise with 5G wireless communications. According to Balaprakash, a scientific problem called Max-Cut can be used to model how

different wireless devices talk to each other at the same time with minimum interference between them. Solving such problems at scale is challenging, yet is important for optimal wireless spectrum management.

Using machine learning to optimize the quantum algorithm involves training it with "rewards" and "penalties" depending on how well it performs, said Sami Khairy, a study author and graduate student at the Illinois Institute of Technology. "It's an iterative procedure that allows us to improve how the computation is running," he said. "It learns a better way to assign new parameters, and we want to assign good parameters as fast as possible."

One of the big advantages of doing this kind of machine learning involves the ability to generalize the principles of the findings over the broader class of problem instances, Khairy explained. "We've designed an optimization algorithm that works for several instances," he said. "In previous studies, it was as if we were training one driver to drive one kind of car; here, we have the ability to train our driver to adapt to many different kinds of cars, in real time."

11 Cosmic rays may soon stymie quantum computing

by Massachusetts Institute of Technology

https://phys.org/news/2020-08-cosmic-rays-stymie-quantum.html

The practicality of quantum computing hangs on the integrity of the quantum bit, or qubit.

Qubits, the logic elements of quantum computers, are coherent two-level systems that represent quantum information. Each qubit has the strange ability to be in a quantum superposition, carrying aspects of both states simultaneously, enabling a quantum version of parallel computation. Quantum computers, if they can be scaled to accommodate many qubits on one processor, could be dizzyingly faster, and able to handle far more complex problems, than today's conventional computers.

But that all depends on a qubit's integrity, or how long it can operate before its superposition and the quantum information are lost – a process called decoherence, which ultimately limits the computer runtime. Superconducting qubits – a leading qubit modality today – have achieved exponential improvement in this key metric, from less than one nanosecond in 1999 to around 200 microseconds today for the best-performing devices.

But researchers at MIT, MIT Lincoln Laboratory, and Pacific Northwest National Laboratory (PNNL) have found that a qubit's performance will soon hit a wall. In a paper published in Nature, the team reports that the low-level, otherwise harmless background radiation that is emitted by trace elements in concrete walls and incoming cosmic rays are enough to cause decoherence in qubits. They found that this effect, if left unmitigated, will limit the performance of qubits to just a few milliseconds.

Given the rate at which scientists have been improving qubits, they may hit this radiation-induced wall in just a few years. To overcome this barrier, scientists will have to find ways to shield qubits – and any practical quantum computers – from low-level radiation, perhaps by building the computers underground or designing qubits that are tolerant to radiation's effects.

"These decoherence mechanisms are like an onion, and we've been peeling back the layers for past 20 years, but there's another layer that left unabated is going to limit us in a couple years, which is environmental radiation," says William Oliver, associate professor of electrical engineering and computer science and Lincoln Laboratory Fellow at MIT. "This is an exciting result, because it motivates us to think

of other ways to design qubits to get around this problem."

The paper's lead author is Antti Vepsäläinen, a postdoc in MIT's Research Laboratory of Electronics.

"It is fascinating how sensitive superconducting qubits are to the weak radiation. Understanding these effects in our devices can also be helpful in other applications such as superconducting sensors used in astronomy," Vepsäläinen says.

⋮

25 Aug 2020

12 Introducing the Qiskit Challenge India, A Taste of Quantum Machine Learning for Qiskitters in India

by Rana Prathap Simh Mukthavaram

https://medium.com/qiskit/introducing-the-qiskit-india-challenge-a-taste-of-quantum-machine-learning-for-qiskitters-in-india-4780ddbb03ab

Qiskit Challenge 2019 was my ticket into the quantum computing world. This year, the Qiskit team wants to bring the same opportunity exclusively to India's aspiring quantum pioneers.

On Tuesday, September 1st, we'll be kicking off a two-week-long event: Qiskit Challenge India. I'm excited to present this opportunity for quantum computing-interested folks in India to meet other Qiskitters and IBMers, learn the fundamentals of quantum computing, and tackle an open problem in the budding field of quantum machine learning.

I first encountered quantum computing in my second year studying Mathematics and Computing at IIT Kharagpur, when I read an article about quantum effects arising in transistors due to their decreasing size and how we could harness rather than avoid them to speed up computations. Whether or not it was technically correct, it seemed cool and immediately sparked my interest. The next summer, I interned at the University of Calgary, where I worked on a quantum hardware problem: building a quantum random number generator. Working with qubits as a unit of information storage got me interested in learning about what could be done with them in computational devices, re-charting my career trajectory toward quantum computing in the process.

At the same time, I started learning slowly by taking edX courses and playing around with Qiskit, where I found the resources to kick off my journey – and heard about the 2019 Challenge. Even though it was already three weeks into the four-week competition, I randomly reached out to another member of the Qiskit community who I'd never met before but who seemed to know a lot about quantum computing, Rahul Pratap Singh, and asked if he'd like to partner up. I'm so happy that I did.

We dove in, rereading all of the material that the IBM Quantum team had released in the past three weeks, learning about quantum computers and gates while we answered previous questions. But then we got to this amazing question: it was a graph coloring problem depicted through a story about a city with Japanese convenience stores called konbinis which we had to color such that no two adjacent stores had the same color. The story disguised the fact that we were actually working on an important mathematical problem on a quantum computer. We worked for three to four days trying to figure out the solution, and stayed up all night. It was invigorating. We noticed that we were behind in the leaderboard, so I took a

small risk, one I thought was right on the verge of breaking the competition's rules, and submitted it. We placed third.

A few days later, the competition's organizer Yuri Kobayashi reached out to tell us that, while our solution was incredibly efficient, it didn't conform to the rules, and so we were removed from the leaderboard. But the judges liked our work so much that we were invited to Qiskit Camp Asia. That experience was eye-opening. I realized that the quantum computing community was vast and much bigger than I expected. During the camp I had a conversation with a Ph.D student on a bus ride, and he explained a lot of what I wanted to know about his field of study, quantum error correction. I also witnessed just how many resources IBM had invested in the community to make a seemingly opaque area like quantum computing more accessible. Mainly, this entire experience gave me perspective on the different sub-fields of quantum computing research. I realized that you did not need a Ph.D in physics to work in quantum computing, and you could contribute significantly as a mathematician like me. This made me want to pursue a full-time career in quantum computing.

I've since joined the IBM Quantum and Qiskit team (where Rahul and I are coworkers, by the way) and now, I want to give back to the quantum community in India. Considering that I got into quantum computing through a competition, I thought that it would be a great opportunity for quantum novices to experience quantum computing the way I had: through a competition solving a real-world problem on a quantum computer.

This brings me to the Qiskit Challenge India. The challenge will begin with simple exercises to help you get your hands dirty, but the final question will require teamwork and possibly long hours of brainstorming. I picked Quantum Machine Learning (QML) as the challenge's focus because I wanted to learn about this exciting new topic alongside you, the challenge's participants. However, QML is still in its early stages, and it's unclear just how good a speedup it will provide over classical machine learning in the near term. This challenge will be an opportunity for you to work on an open problem in QML today – one where we still don't know what the best answer is. The best part is that you don't need any prior knowledge in quantum computing, just a basic working knowledge of python.

My advice for you is to use this opportunity to interact with the community. It's a team challenge, and working together will help you learn far faster than working on your own. Ask questions shamelessly, and use this as a way to get to know fellow Qiskitters, Qiskit Advocates, and IBMers. I hope that you'll take part!

13 Researchers on a path to build powerful and practical quantum computer

by The Optical Society

https://phys.org/news/2020-08-path-powerful-quantum.html

For the first time, researchers have designed a fully connected 32-qubit trapped-ion quantum computer register operating at cryogenic temperatures. The new system represents an important step toward developing practical quantum computers.

Junki Kim from Duke University will present the new hardware design at the inaugural OSA Quantum 2.0 conference to be co-located as an all-virtual event with OSA Frontiers in Optics and Laser Science APS/DLS (FiO + LS) conference 14-17 September.

Instead of using traditional computer bits that can only be a zero or a one, quantum computers use qubits that can be in a superposition of computational states. This allows quantum computers to solve problems that are too complex for traditional computers.

Trapped-ion quantum computers are among the most promising type of quantum technology for quantum computing, but it has been challenging to create these computers with enough qubits for practical use.

"In collaboration with the University of Maryland, we have designed and constructed several generations of fully-programmable ion trap quantum computers," said Kim. "This system is the latest in the effort where many of the challenges leading to long-term reliability is tackled head-on."

Scaling up quantum computers

Trapped-ion quantum computers cool ions to extremely low temperatures, which allows them to be suspended in an electromagnetic field in an ultra-high vacuum and then manipulated with precise lasers to form qubits.

Thus far, achieving high computational performance in large-scale ion trap systems has been hampered by the collisions with background molecules disrupting the ion chain, instability of the laser beams driving the logic gates seen by the ion, and electric field noise from the trapping electrodes agitating the ion's motion often used to create entanglement.

In the new work, Kim and colleagues addressed these challenges by incorporating dramatically new approaches. The ions are trapped in a localized ultra-high vacuum enclosure inside a closed-cycle cryostat cooled to 4K temperatures, with minimal vibrations. This arrangement eliminates the disturbance of the qubit chain arising from collisions with residual molecules from the environment, and strongly suppresses the anomalous heating from the trap surface.

To achieve clean laser beam profiles and minimize errors, the researchers used a photonic crystal fiber to connect various parts of the Raman optical system that drives qubit gates – the building blocks of quantum circuits. In addition, the delicate laser systems needed to operate the quantum computers are engineered to be taken off the optical table and installed in instrument racks. The laser beams are then delivered to the system in single-mode optical fibers. They embraced new ways of designing and implementing optical systems that fundamentally eliminate mechanical and thermal instabilities to create a turn-key laser setup for trapped ion quantum computers.

The researchers have demonstrated that the system is capable of automated on-demand loading of ion qubit chains, and can perform simple qubit manipulations using microwave fields. The team is making solid progress towards implementing entangling gates, in a manner that can scale up to full 32 qubits.

In future work, and in collaboration with computer scientists and quantum algorithm researchers, the team plans to integrate hardware-specific software with the trapped-ion quantum computing hardware. The fully integrated system, composed of fully-connected trapped-ion qubits and hardware-specific software, will lay a foundation for practical trapped-ion quantum computers.

24 Aug 2020

14 What Intel is Planning for The Future of Quantum Computing: Hot Qubits, Cold Control Chips, and Rapid Testing

by Samuel K. Moore

https://spectrum.ieee.org/tech-talk/computing/hardware/intels-quantum-computing-plans-hot-qubits-cold-control-chips-and-rapid-testing?utm_source=techalert&utm_medium=email&utm_campaign=techalert-08-27-20&mkt_tok=eyJpIjoiWXpjMk1tSTFaamRoWXpGaiIsInQiOiI3VUF1cmpXYkVmd0NDeVwvcFwvVWtFRGNhcEZETnR6RGxzamVsV2syb3hTYnpPZmY5VHdHQklSRO5tRk8x

Quantum computing may have shown its "supremacy" over classical computing a little over a year ago, but it still has a long way to go. Intel's director of quantum hardware, Jim Clarke, says that quantum computing will really have arrived when it can do something unique that can change our lives, calling that point "**quantum practicality**." Clarke talked to IEEE Spectrum about how he intends to get silicon-based quantum computers there:

IEEE Spectrum: Intel seems to have shifted focus from quantum computers that rely on superconducting qubits to ones with silicon spin qubits. Why do you think silicon has the best chance of leading to a useful quantum computer?

Jim Clarke: It's simple for us . . . Silicon spin qubits look exactly like a transistor. . . . The infrastructure is there from a tool fabrication perspective. We know how to make these transistors. So if you can take a technology like quantum computing and map it to such a ubiquitous technology, then the prospect for developing a quantum computer is much clearer.

I would concede that today silicon spin-qubits are not the most advanced quantum computing technology out there. There has been a lot of progress in the last year with superconducting and ion trap qubits.

But there are a few more things: A silicon spin qubit is the size of a transistor – which is to say it is roughly 1 million times smaller than a superconducting qubit. So if you take a relatively large superconducting chip, and you say "how do I get to a useful number of qubits, say 1000 or a million qubits?" all of a sudden you're dealing with a form factor that is . . . intimidating.

We're currently making server chips with billions and billions of transistors on them. So if our spin qubit is about the size of a transistor, from a form-factor and energy perspective, we would expect it to scale much better.

What are silicon spin-qubits and how do they differ from competing technology, such as superconducting qubits and ion trap systems?

In an ion trap you are basically using a laser to manipulate a metal ion through its excited states where the population density of two excited states represents the zero and one of the qubit. In a superconducting circuit, you are creating the electrical version of a nonlinear LC (inductor-capacitor) oscillator circuit, and you're using the two lowest energy levels of that oscillator circuit as the zero and one of your qubit. You use a microwave pulse to manipulate between the zero and one state.

We do something similar with the spin qubit, but it's a little different. You turn on a transistor, and you have a flow of electrons from one side to another. In a silicon spin qubit, you essentially trap a single electron in your transistor, and then you put the whole thing in a magnetic field [using a superconducting electromagnet in a refrigerator]. This orients the electron to either spin up or spin down. We are essentially using its spin state as the zero and one of the qubit.

That would be an individual qubit. Then with very good control, we can get two separated electrons

in close proximity and control the amount of interaction between them. And that serves as our two-qubit interaction.

So we're basically taking a transistor, operating at the single electron level, getting it in very close proximity to what would amount to another transistor, and then we're controlling the electrons.

Does the proximity between adjacent qubits limit how the system can scale?

I'm going to answer that in two ways. First, the interaction distance between two electrons to provide a two-qubit gate is not asking too much of our process. We make smaller devices every day at Intel. There are other problems, but that's not one of them.

Typically, these qubits operate on a sort of a nearest neighbor interaction. So you might have a two-dimensional grid of qubits, and you would essentially only have interactions between one of its nearest neighbors. And then you would build up [from there]. That qubit would then have interactions with its nearest neighbors and so forth. And then once you develop an entangled system, that's how you would get a fully entangled 2D grid. [Entanglement is a condition necessary for certain quantum computations.]

What are some of the difficult issues right now with silicon spin qubits?

By highlighting the challenges of this technology, I'm not saying that this is any harder than other technologies. I'm prefacing this, because certainly some of the things that I read in the literature would suggest that qubits are straightforward to fabricate or scale. Regardless of the qubit technology, they're all difficult.

With a spin qubit, we take a transistor that normally has a current of electrons go through, and you operate it at the single electron level. This is the equivalent of having a single electron, placed into a sea of several hundred thousand silicon atoms and still being able to manipulate whether it's spin up or spin down.

So we essentially have a small amount of silicon, we'll call this the channel of our transistor, and we're controlling a single electron within that that piece of silicon. The challenge is that silicon, even a single crystal, may not be as clean as we need it. Some of the defects – these defects can be extra bonds, they can be charge defects, they can be dislocations in the silicon – these can all impact that single electron that we're studying. This is really a materials issue that we're trying to solve.

Just briefly, what is **coherence time** and what's its importance to computing?

The coherence time is the window during which information is maintained in the qubit. So, in the case of a silicon spin qubit, it's how long before that electron loses its orientation, and randomly scrambles the spin state. It's the operating window for a qubit.

Now, all of the qubit types have what amounts to coherence times. Some are better than others. The coherence times for spin qubits, depending on the type of coherence time measurement, can be on the order of milliseconds, which is pretty compelling compared to other technologies.

What needs to happen [to compensate for brief coherence times] is that we need to develop an error correction technique. That's a complex way of saying we're going to put together a bunch of real qubits and have them function as one very good logical qubit.

How close is that kind of error correction?

It was one of the four items that really needs to happen for us to realize a quantum computer that I wrote about earlier. The first is we need better qubits. The second is we need better interconnects. The third is we need better control. And the fourth is we need error correction. We still need improvements on the first three before we're really going to get, in a fully scalable manner, to error correction.

You will see groups starting to do little bits of error correction on just a few qubits. But we need better qubits and we need a more efficient way of wiring them up and controlling them before you're really going to see fully fault-tolerant quantum computing.

One of the improvements to qubits recently was the development of "hot" silicon qubits. Can you explain their significance?

Part of it equates to control.

Right now you have a chip at the bottom of a dilution refrigerator, and then, for every qubit, you have several wires that that go from there all the way outside of the fridge. And these are not small wires; they're coax cables. And so from a form factor perspective and a power perspective – each of these wires dissipates power – you really have a scaling problem.

One of the things that Intel is doing is that we are developing control chips. We have a control chip called Horse Ridge that's a conventional CMOS chip that we can place in the fridge in close proximity to our qubit chip. Today that control chip sits at 4 kelvins and our qubit chip is at 10 millikelvins and we still have to have wires between those two stages in the fridge.

Now, imagine if we can operate our qubit slightly warmer. And by slightly warmer, I mean maybe 1 kelvin. All of a sudden, the cooling capacity of our fridge becomes much greater. The cooling capacity of our fridge at 10 millikelvin is roughly a milliwatt. That's not a lot of power. At 1 Kelvin, it's probably a couple of Watts. So, if we can operate at higher temperatures, we can then place control electronics in very close proximity to our qubit chip.

By having hot qubits we can co-integrate our control with our qubits, and we begin to solve some of the wiring issues that we're seeing in today's early quantum computers.

Are hot qubits structurally the same as regular silicon spin qubits?

Within silicon spin qubits there are several different types of materials, some are what I would call silicon MOS type qubits – very similar to today's transistor materials. In other silicon spin qubits you have silicon that's buried below a layer of silicon germanium. We'll call that a buried channel device. Each have their benefits and challenges.

We've done a lot of work with TU Delft working on a certain type of [silicon MOS] material system, which is a little different than most in the community are studying [and lets us] operate the system at a slightly higher temperature.

I loved the quantum supremacy work. I really did. It's good for our community. But it's a contrived problem, on a brute force system, where the wiring is a mess (or at least complex).

What we're trying to do with the hot qubits and with the Horse Ridge chip is put us on a path to scaling that will get us to a useful quantum computer that will change your life or mine. We'll call that quantum practicality.

What do you think you're going to work on next most intensely?

In other words, “What keeps Jim up at night?”

There are a few things. The first is time-to-information. Across most of the community, we use these dilution refrigerators. And the standard way [to perform an experiment] is: You fabricate a chip; you put it in a dilution refrigerator; it cools down over the course of several days; you experiment with it over the course of several weeks; then you warm it back up and put another chip in.

Compare that to what we do for transistors: We take a 300-millimeter wafer, put it on a probe station, and after two hours we have thousands and thousands of data points across the wafer that tells us something about our yield, our uniformity, and our performance.

That doesn’t really exist in quantum computing. So we asked, “Is there way to – at slightly higher temperatures – to combine a probe station with a dilution refrigerator?” Over the last two years, Intel has been working with two companies in Finland [Bluefors Oy and Afore Oy] to develop what we call the cryoprober. And this is just coming online now. We’ve been doing an impressive job of installing this massive piece of equipment in the complete absence of field engineers from Finland due to the Coronavirus.

What this will do is speed up our time-to-information by a factor of up to 10,000. So instead of wire bonding a single sample, putting it in the fridge, taking a week to study it, or even a few days to study it, we’re going to be able to put a 300-millimeter wafer into this unit and over the course of an evening step and scan. So we’re going to get a tremendous increase in throughput. I would say a 100× improvement. My engineers would say 10,000. I’ll leave that as a challenge for them to impress me beyond the 100.

Here’s the other thing that keeps me up at night. Prior to starting the Intel quantum computing program, I was in charge of interconnect research in Intel’s Components Research Group. (This is the wiring on chips.) So, I’m a little less concerned with the wiring into and out of the fridge than I am just about the wiring on the chip.

I’ll give an example: An Intel server chip has probably north of 10 billion transistors on a single chip. Yet the number of wires coming off that chip is a couple of thousand. A quantum computing chip has more wires coming off the chip than there are qubits. This was certainly the case for the Google [quantum supremacy] work last year. This was certainly the case for the Tangle Lake chip that Intel manufactured in 2018, and it’s the case with our spin qubit chips we make now.

So we’ve got to find a way to make the interconnects more elegant. We can’t have more wires coming off the chip than we have devices on the chip. It’s ineffective.

This is something the conventional computing community discovered in the late 1960s with Rent’s Rule [which empirically relates the number of interconnects coming out of a block of logic circuitry to the number of gates in the block]. Last year we published a paper with Technical University Delft on the quantum equivalent of Rent’s Rule. And it talks about, amongst other things the Horse Ridge control chip, the hot qubits, and multiplexing.

We have to find a way to multiplex at low temperatures. And that will be hard. You can’t have a million-qubit quantum computer with two million coax cables coming out of the top of the fridge.

Doesn’t Horse Ridge do multiplexing?

It has multiplexing. The second generation will have a little bit more. The form factor of the wires [in the new generation] is much smaller, because we can put it in closer proximity to the [quantum] chip.

So if you kind of combine everything I’ve talked about. If I give you a package that has a classical control chip – call it a future version of Horse Ridge – sitting right next to and in the same package as a

quantum chip, both operating at a similar temperature and making use of very small interconnect wires and multiplexing, that would be the vision.

What's that going to require?

It's going to require a few things. It's going to require improvements in the operating temperature of the control chip. It's probably going to require some novel implementations of the packaging so there isn't a lot of thermal cross talk between the two chips. It's probably going to require even greater cooling capacity from the dilution refrigerator. And it's probably going to require some qubit topology that facilitates multiplexing.

Given the significant technical challenges you've talked about here, how optimistic are you about the future of quantum computing?

At Intel, we've consistently maintained that we are early in the quantum race. Every major change in the semiconductor industry has happened on the decade timescale and I don't believe quantum will be any different. While it's important to not underestimate the technical challenges involved, the promise and potential are real. I'm excited to see and participate in the meaningful progress we're making, not just within Intel but the industry as a whole. A computing shift of this magnitude will take technology leaders, scientific research communities, academia, and policy makers all coming together to drive advances in the field, and there is tremendous work already happening on that front across the quantum ecosystem today.

15 Bridgefy, the messenger promoted for mass protests, is a privacy disaster

by DAN GOODIN

https://arstechnica.com/features/2020/08/bridgefy-the-app-promoted-for-mass-protests-is-a-privacy-disaster/

The rise of mass protests over the past year – in Hong Kong, India, Iran, Lebanon, Zimbabwe, and the US – has presented activists with a major challenge. How do you communicate with one another when Internet connections are severely congested or completely shut down and at the same time keep your identity and conversations private?

One heavily promoted solution has been **Bridgefy**, a messaging app that has the financial and marketing backing of Twitter cofounder Biz Stone and boasts having more than 1.7 million installations. By using Bluetooth and mesh network routing, Bridgefy lets users within a few hundred meters – and much further as long as there are intermediary nodes – to send and receive both direct and group texts with no reliance on the Internet at all.

Bridgefy cofounder and CEO Jorge Ríos has said he originally envisioned the app as a way for people to communicate in rural areas or other places where Internet connections were scarce. And with the past year's upswell of large protests around the world – often in places with hostile or authoritarian governments – company representatives began telling journalists that the app's use of end-to-end encryption (reiterated here, here, and here) protected activists against governments and counter protesters trying to intercept texts or shut down communications.

Over the past few months, the company has continued to hold out the app as a safe and reliable way for activists to communicate in large gatherings. Bridgefy's tweets embrace protestors in Belarus, India,

and Zimbabwe, not to mention the Black Lives Matter protests throughout the US. The company has also said its software developer kit can be used to build COVID-19 contact tracing apps.

Just this month, on August 10, this article quoted Bridgefy cofounder and CEO Jorge Ríos saying: "Last year, we became the protest app." Up until last week, Bridgefy told Android users via the Google Play Store, "Don't worry! Your messages are safe and can't be read by those people in the middle." The company continues to encourage iOS users to "have secure and private conversations" using the app.

But now, researchers are revealing a litany of recently uncovered flaws and weaknesses that show that just about every claim of anonymity, privacy, and reliability is outright false.

Unsafe at any speed

In a paper published on Monday, researchers said that the app's design for use at concerts, sports events, or during natural disasters makes it woefully unsuitable for more threatening settings such as mass protests. They wrote:

> Though it is advertised as "safe" and "private" and its creators claimed it was secured by end-to-end encryption, none of aforementioned use cases can be considered as taking place in adversarial environments such as situations of civil unrest where attempts to subvert the application's security are not merely possible, but to be expected, and where such attacks can have harsh consequences for its users. Despite this, the Bridgefy developers advertise the app for such scenarios and media reports suggest the application is indeed relied upon.

The researchers are: Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Marekova from Royal Holloway, University of London. After reverse engineering the app, they devised a series of devastating attacks that allow hackers – in many cases with only modest resources and moderate skill levels – to take a host of nefarious actions against users. The attacks allow for:

- deanonymizing users
- building social graphs of users' interactions, both in real time and after the fact
- decrypting and reading direct messages
- impersonating users to anyone else on the network
- completely shutting down the network
- performing active man-in-the-middle attacks, which allow an adversary not only to read messages, but to tamper with them as well

Impersonation, MitMs, and more

A key shortcoming that makes many of these attacks possible is that Bridgefy offers no means of cryptographic authentication, which one person uses to prove she's who she claims to be. Instead, the app relies on a user ID that's transmitted in plaintext to identify each person. Attackers can exploit this by sniffing the ID over the air and using it to spoof another user.

With no effective way to authenticate, any user can impersonate any other user, as long as an attacker has come into contact with that user (either one-on-one or in network-wide broadcast messages) at least once. With that, the attacker can pose as a trusted contact and trick a person into revealing personal names or other confidential information, or take harmful actions. The lack of authentication can also give rise to eavesdropping or tampering of messages.

Here's how: When hypothetical Bridgefy user Ursula messages Ivan, she uses Ivan's public key to encrypt the message. Ivan then uses his private key to decrypt the message. With no cryptographic means to verify a user's identity, an attacker – say, one named Eve – can impersonate Ivan and present her own public key to Ursula. From then on, Eve can intercept and read all messages Ursula sends to Ivan. To tamper with the messages Ursula or Ivan send, Eve impersonates both parties to the other. With that, Eve can intercept the messages each sends and change the contents or add malicious attachments before sending it on to the other party.

There's a separate way to read encrypted messages, thanks to another major Bridgefy flaw: its use of PKCS #1, an outdated way of encoding and formatting messages so that they can be encrypted with the RSA cryptographic algorithm. This encoding method, which was deprecated in 1998, allows attackers to perform what's known as a padding oracle attack to derive contents of an encrypted message.

16 Microsoft to train 900 Indian teachers in Quantum Computing

by Education Desk

https://indianexpress.com/article/education/microsoft-to-train-900-indian-teachers-in-quantum-computing-6567698/

Microsoft is creating a new programme to build quantum computing skills and capabilities in the academic community in India. As part of this initiative, Microsoft Garage is organising a 'Train the Trainer' programme in collaboration with Electronics and ICT Academies at Malaviya National Institute of Technology (MNIT), Jaipur and National Institute of Technology, Patna, the tech giant claims.

This programme will train 900 faculty from universities and institutes across India at institutes of national importance including IIT-Kanpur, IIT-Guwahati, IIT-Roorkee, MNIT Jaipur, NIT-Patna, IIIT-D Jabalpur, and NIT Warangal, claims Microsoft India in an official statement.

Quantum computers will enable new discoveries in the areas of healthcare, energy, environmental systems, smart materials, and beyond. The training programme will be conducted virtually, from August 24 - 29, 2020. The programme will also cover practical coding for participants using Microsoft Q# & Quantum Development Kit, claims the tech giant.

Key themes that will be covered include – an introduction to quantum information, quantum concepts such as superposition and entanglement, processing of information using qubits and quantum gates, as well as an introduction to quantum machine learning and quantum programming.

Rajiv Kumar, Managing Director, Microsoft India Development Center, and Corporate Vice President, Enterprise+Devices India, said, "India is renowned across the world for its science, technology, engineering, mathematics and computing (STEM+C) workforce, and a tech-capable citizenry. Through this initiative in India, we aim to develop skills in quantum at scale, which has the potential to trigger the new frontier of innovation, shaping the future of the IT industry in this part of the world."

Reena Dayal, Director, Microsoft Garage India and Chair for IEEE Quantum SIG, said, "Quantum

computing holds the potential to solve some of the most pressing issues our world faces today. Through this program, we aim to equip academia in India with the requisite knowledge to develop a comprehensive quantum learning curriculum in their institutions and help develop these skills among some of the brightest minds in the country."

17 Algorithm May Be Able to Predict Power of Early Quantum Computers

by Matt Swayne

https://thequantumdaily.com/2020/08/24/algorithm-may-be-able-to-predict-power-of-early-quantum-computers/

Quantum physicists at the University of Sussex have created an algorithm that speeds up the rate of calculations in the early quantum computers which are currently being developed. They have created a new way to route the ions – or charged atoms – around the quantum computer to boost the efficiency of the calculations.

The Sussex team have shown how calculations in such a quantum computer can be done most efficiently, by using their new 'routing algorithm'. Their paper "Efficient Qubit Routing for a Globally Connected Trapped Ion Quantum Computer" is published in the journal Advanced Quantum Technologies.

The team working on this project was led by Professor Winfried Hensinger and included Mark Webber, Dr Steven Herbert and Dr Sebastian Weidt. The scientists have created a new algorithm which regulates traffic within the quantum computer just like managing traffic in a busy city. In the trapped ion design the qubits can be physically transported over long distances, so they can easily interact with other qubits. Their new algorithm means that data can flow through the quantum computer without any 'traffic jams'. This in turn gives rise to a more powerful quantum computer.

Quantum computers are expected to be able to solve problems that are too complex for classical computers. Quantum computers use quantum bits (qubits) to process information in a new and powerful way. The particular quantum computer architecture the team analyzed first is a 'trapped ion' quantum computer, consisting of silicon microchips with individual charged atoms, or ions, levitating above the surface of the chip. These ions are used to store data, where each ion holds one quantum bit of information. Executing calculations on such a quantum computer involves moving around ions, similar to playing a game of Pacman, and the faster and more efficiently the data (the ions) can be moved around, the more powerful the quantum computer will be.

In the global race to build a large scale quantum computer there are two leading methods, 'superconducting' devices which groups such as IBM and Google focus on, and 'trapped ion' devices which are used by the University of Sussex's Ion Quantum Technology group, and the newly emerged company Universal Quantum, among others.

Superconducting quantum computers have stationary qubits which are typically only able to interact with qubits that are immediately next to each other. Calculations involving distant qubits are done by communicating through a chain of adjacent qubits, a process similar to the telephone game (also referred to as 'Chinese Whispers'), where information is whispered from one person to another along a line of people. In the same way as in the telephone game, the information tends to get more corrupted the longer the chain is. Indeed, the researchers found that this process will limit the computational power of superconducting quantum computers.

In contrast, by deploying their new routing algorithm for their trapped ion architecture, the Sussex scientists have discovered that their quantum computing approach can achieve an impressive level of computational power. 'Quantum Volume' is a new benchmark which is being used to compare the computational power of near term quantum computers. They were able to use Quantum Volume to compare their architecture against a model for superconducting qubits, where they assumed similar levels of errors for both approaches. They found that the trapped-ion approach performed consistently better than the superconducting qubit approach, because their routing algorithm essentially allows qubits to directly interact with many more qubits, which in turn gives rise to a higher expected computational power.

Mark Webber, a doctoral researcher in the Sussex Centre for Quantum technologies, at the University of Sussex, said:

"We can now predict the computational power of the quantum computers we are constructing. Our study indicates a fundamental advantage for trapped ion devices, and the new routing algorithm will allow us to maximize the performance of early quantum computers."

Professor Hensinger, director of the Sussex Centre for Quantum Technologies at the University of Sussex said:

"Indeed, this work is yet another stepping stone towards building practical quantum computers that can solve real world problems."

Professor Winfried Hensinger and Dr Sebastian Weidt have recently launched their spin-out company **Universal Quantum** which aims to build the world's first large scale quantum computer. It has attracted backing from some of the world's most powerful tech investors. The team was the first to publish a blue-print for how to build a large scale trapped ion quantum computer in 2017.

21 Aug 2020

18 Quantum Technology based Banking Security enters in South Korean Market

by ALVIN HOLT

https://morningtick.com/2020/08/21/quantum-technology-based-banking-security-enters-in-south-korean-market/

SK Technologies announced the first quantum security-based financial services on 5G smartphones on August 20, 2020. The company plans to employ this technology to DGB Daegu Bank's mobile banking app, 'IM Bank'. This is the first time that quantum security is available for banking services on 5G smartphones.

It can be fairly concluded that SK Technologies had the lion's share in this feat. They worked with Samsung to develop the 'Samsung Galaxy A Quantum' 5G smartphone early in 2020; quantum security banking is a dedicated service for this device.

Where does Quantum security tech work?

Quantum security tech is at work during the process of receiving OTPs from banking institutions. Customers receive these one-time-passwords on their personal devices. The tech will also work during the

opening of bank accounts since that process deals with much personal information. A third-party hack during these processes can be extremely harmful.

According to the press release issued by SK Tech, "Usually, digital OTP number and ID card authentication information are transmitted to the server of DGB Daegu Bank and KFTC after the encryption process. If a third party hacks this password, enormous damage can occur."

How does Quantum security tech work?

The Quantum security tech developed by SK Tech will work on the DGB Daegu Bank's 'IM Bank' app. This is DGB Daegu's mobile banking app. The Samsung Galaxy A Quantum smartphone has the QRNG (Quantum Random Number Generation) chipset embedded in it by SK Tech. This allows the smartphone to generate complex encryption on the IM Bank app during the aforementioned risky processes.

SK Tech said, "SK Telecom's Quantum Random Number Generation (QRNG) chipset mounted on the Galaxy A Quantum creates unpredictable and patternless pure random numbers using the randomness of the quantum. Based on this random number, it is a principle that improves security by encrypting the digital OTP number and identification information of the 'IM Bank' app."

Why is Quantum security tech used?

Online and digital banking numbers are increasing due to the ongoing Covid-19 pandemic. 'Non face-to-face' transactions are also rising, which will only lead to an increase in the risk of financial fraud. According to the Financial Supervisory Service, the number of victims of voice phishing crimes in 2019 was 672 billion won, a 51% increase from 2018.

Quantum security technology will pave the way toward preventing financial fraud. SK Technologies is also planning to collaborate with other financial institutions to use the Quantum security tech and prevent frauds.

According to SK Tech's Korean press release, the collaboration with DGB Daegu Bank will be in action from the middle of next month.

Speaking about the achievement, Myung-jin Han, head of SK Telecom's MNO Marketing Group, said, "Since the launch of the world's first quantum security smartphone in May last year, sales have continued to be strong, and quantum security has been expanded to various services. It will converge in various fields such as IoT (Internet of Things)."

20 Aug 2020

19 US Army announces a 128-qubit prototype project

https://www.swissquantumhub.com/us-army-announces-a-128-qubit-prototype-projet/

A research project funded by the U.S. Army has developed a new approach to manufacturing quantum computer chips, representing a significant step forward toward making quantum processors.

The research was completed by scientists at the Massachusetts Institute of Technology and Sandia National Laboratories on the behalf of the Army Research Laboratory.

In this study, researchers succeeded in integrating 128 qubits onto a photonic chip by making small quantum "chiplets" and placing them onto a larger circuit. The chiplets were able to carry quantum information through artificial atoms created by scientists by exploiting defects in diamonds.

The new technology still needs to undergo tests to ensure the qubits in the chip can be controlled easily.

20 How to Ensure the U.S.'s Quantum Future

by Dario Gil

https://www.scientificamerican.com/article/how-to-ensure-the-uss-quantum-future/

Science knows no borders. Fundamental research, done by domestic or foreign talent, underpins progress and drives innovation – and ultimately, improves our lives. Continuing to attract foreign highly skilled scientists to the United States and retaining them is crucial for building a bright future that relies on emerging technologies such as **quantum computing** and **artificial intelligence (AI)**.

We need these scientists – and we need them badly.

Over the years, foreign-born physicists, chemists, computer scientists, mathematicians, you name it, have been contributing greatly to the U.S. leadership in quantum and AI. Just look at IBM Research. IBM is an American company with a global footprint, and in the U.S. we have three research labs – in Yorktown Heights, N.Y., Almaden, Calif., and Cambridge, Mass. Among our AI-skilled researchers, 58% are from abroad. In quantum computing, it's a quarter of our workforce. And in cloud, another important area for us, it's 55% of our research community.

I am the director of IBM Research. When I speak, I speak with an accent, just like all of my foreign-born colleagues. I was born in Spain and came to the U.S. as a teenager. I finished my last year of high school here in 1993, at Los Altos High near Palo Alto, Calif., and loved the country so much that I decided to stay. Ever since, I've been working to make America a better place to live, having graduated from MIT with a Ph.D. in electrical engineering and computer science. I promised myself then to give my wit, education, dedication and passion to this country, my new home.

My case is far from unique. America has long been called the Land of Opportunity. But every individual opportunity yields dividends for the whole nation. Talent is the most critical resource in today's knowledge economy. We must prioritize the development, attraction and retention of highly skilled workers. A declining birth rate, the ever-changing nature of work that increasingly demands STEM skills, and not enough STEM training at home – a problem we must urgently address – means the U.S. must remain a beacon to attract the best global talent. Nations that understand the importance of developing, attracting and retaining human capital will be uniquely positioned to create the best future and benefit from the advancements in science and technology.

Our world has not run out of problems to solve – from pandemics to climate change to creating economic opportunity for all. The urgency of science has never been greater.

Make no mistake. While emerging technologies like AI and quantum are absolutely crucial for our economy, society and the continuous progress of our country, it is top talent that makes the U.S. a world leader in these, and many other, areas. And it's top talent that is in short supply. MIT's President Rafael Reif put it quite bluntly in a recent New York Times opinion piece. "Why is foreign talent so important to the United States? For the same reason the Boston Red Sox don't limit themselves to players born in

Boston: The larger the pool you draw from, the larger the supply of exceptional talent," he argued. "By challenging, inspiring and stretching one another, they make one another better, just as star players raise a whole team's level of play."

Take quantum. This technology of the near future is set to revolutionize the world of computing and will likely deeply impact our society and economy. Having been confined to research labs for years, it's finally emerging as a nascent industry. For specific tasks, quantum computers promise to unlock processing power much superior to traditional, classical, computers. With continued progress, they should be able to perform calculations and generate simulations of unprecedented complexity at a fraction of the time it would take a classical computer. They should even be able to deal with problems a classical computer could never solve. The implications of quantum for security, chemistry, material design, financial markets, AI and machine learning are immense.

And now look at the people driving this quantum revolution in the U.S.; IBM, Google, Microsoft, Honeywell, Intel and startups like Rigetti and IonQ are all pursuing quantum computing research here in America. At IBM, among the foreign-born quantum researchers is the lead of our quantum program, IBM Fellow Jay Gambetta. An Australian, he has been working in quantum computing for 20 years, having come to the U.S. in 2004 to continue his research studies. He became a citizen last year.

When Gambetta first arrived in the U.S., quantum computing wasn't yet mainstream. It was thanks to foreign-born, highly skilled researchers like him that this country has been able to emerge as a global leader in this crucial area. It was his quantum team, which included IBM Fellow Matthias Steffen – another immigrant and naturalized American – that in 2012 put IBM Research on the global experimental quantum computing map. They created stable superconducting qubits, the building blocks of quantum computers. And four years later, Gambetta and his colleagues became the first in the world to make quantum computers available globally and for free through the cloud – to anyone.

According to a 2019 report by the Center for Security and Emerging Technology (CSET), more than 50% of computer scientists with graduate degrees currently employed in the U.S. were born abroad – and nearly 70% of enrolled computer science graduate students as well. The same report found, though, that the vast majority of this foreign-born talent wants to remain in the U.S. In AI-related fields specifically, around 80% of U.S.-educated Ph.D. graduates have stayed in the country – just like the 58% of foreign-born AI researchers that now work at IBM's American labs.

These stats show that we should keep investing in our highly skilled citizens with vigor and ambition – be they naturalized citizens or citizens by birth. Economic opportunities abroad are rising, and it will soon be increasingly difficult to attract and retain these workers – the workers we so desperately need here in America. We must also consider the security of our research enterprise, particularly when it comes to the countries that do not share our democratic values, respect for human rights, and the rule of the law. But above all, investing in our citizens is simply the right thing to do, as it means we recognize and value the intrinsic potential of the talent present in every corner of our country.

We also need to address the chronic underfunding of historically Black colleges and universities (HBCUs) – great scientific, economic and cultural drivers. They accomplish a lot with very modest investment. Just consider that although only about 9% of America's Black students enroll in HBCUs, roughly 16% of all Black scientists and engineers are their graduates. Imagine what they could achieve with more funding.

Each year, more than 50,000 bachelor's degrees in computer science and related fields are awarded to U.S. citizens or permanent residents. It has been recommended to "staple" green cards to the diplomas of all foreign-born Ph.D.s who graduate in STEM from American universities. Similarly, we should award

graduate fellowships to all U.S. undergraduate majors in computer science with GPAs above a certain level.

Our country and the world are full of talent. We should embrace diversity and foreign highly skilled workers as much as we embrace the emerging technology that they bring us. The skills and passion of our citizens and immigrants are the pillars of strength for advancing the scientific and technological leadership of our nation. As Avi Loeb, the chair of the Astronomy Department at Harvard University, has written in these very pages, science is an infinite-sum game. Diversity is our strength and competitive advantage. It is time to reset America's commitment to science and to raise our level of ambition to ensure our country remains a beacon to, and the home of, the world's best STEM talent.

21 Intro to Decentralized Identity Technology: How Does Blockchain Cryptography Work?

by Katie Lu

https://www.finextra.com/blogposting/19221/intro-to-decentralized-identity-technology-how-does-blockchain-cryptography-work

The most commonly talked about feature of blockchain is that it is decentralized, meaning that there is no single organization or individual in control of all the information. In 2017, as blockchain gained a lot of media attention, critics focused on the public aspect of the platform and said that everybody could see transactions happening. However, that was the case with public blockchains, which have since evolved into different subsets of chains. Below are some main types of blockchains, their users, and purposes.

- **Public blockchain:** The original blockchain that gained attention. Allowed for P2P (peer to peer) transactions, which was a large part of Bitcoin. Any person or company could be a part of it. Examples: Bitcoin, Ethereum
- **Private blockchain:** Allows a number or cap of people that have access to transactions. Mostly attractive for companies because it is most similar to how they currently operate in order to keep data internal. Examples: Hyperledger, R3 Corda
- **Permissioned blockchain:** Similar to private blockchains, except it can also control who is a part of the network and has access, which are further controls on transactions.
- **Hybrid blockchain:** Combines private and public features, with data private but stored on a public blockchain. Example: Dragonchain
- **Federated blockchain:** Similar to private blockchains, but is considered to be highly private with even stricter controls. Allows for more privacy but also better visibility and accountability.

Cryptography behind blockchain

Blockchains are powered by lots of small cryptography primitives. A public/private key pair is one of these building blocks that is key for a self-sovereign identity because no third party is required.

Public-key cryptography, also known as asymmetric cryptography, is any cryptographic system that uses key pairs: a public key that can be disseminated widely, and a private key which is only accessible to the owner. This allows for two functions: **authentication**, where the public key is used to verify that the

holder of the paired private key sent the message; as well as **encryption**, where only the paired private key holder can decrypt the message encrypted with the public key.

These authentication and encryption tools are used to unlock the blockchain.

Decentralized identity

The Decentralized Identity Foundation defines decentralized identities (DIDs) as "anchored by blockchain IDs linked to zero-trust datastores that are universally discoverable", but that only cracks the surface of the potential of DIDs. Breaking down that statement, the three key parts of DID are blockchain IDs, zero-trust datastores, and universally discoverable.

- **Blockchain IDs:** The blockchain, compared to public-key infrastructure alone, cannot be censored or controlled by a central authority. With identification as a big part of today's globalized world, blockchain IDs introduce a new level of security while being borderless.
- **Zero-trust datastores:** A zero-trust datastore has the ability to store private information locally in user devices while maintaining trust and authenticity globally. One way to incorporate zero-trust datastores is to require biometrics to access user data.
- **Universally discoverable:** An important way that this approach saves companies money is that they allow businesses to share verifications. The security is not compromised, as it still requires biometrics to access the data and authentication from the new company accessing the data. All parties can cut costs by re-using secure, stored verification credentials.

Conclusions

Over the last few years, identity related solutions have been on the rise. In fact, an entire ecosystem has been created for helping companies verify their customers and keep track of them in increasingly efficient ways. The only problem with such breakthroughs was that they do not often put the customer first, and they can usually tell. For example, as the people's trust in social media has been undermined by big tech's misuse of their data, they feel less comfortable letting their social media know everything about them. People demand a better solution that works for everyone. New identity technologies solve these concerns, align with Decentralized Identity Foundation standards, and are committed to providing secure, stored decentralized identity solutions. Now is the time to implement solutions, as identity management costs and issues are only rising as technology is used more.

22 IBM hits new quantum computing milestone

by Stephanie Condon

https://www.zdnet.com/article/ibm-hits-new-quantum-computing-milestone/

IBM on Thursday announced it's reached a new quantum computing milestone, hitting its highest Quantum Volume to date. Using a 27-qubit client-deployed system, IBM achieved a Quantum Volume of 64.

Quantum Volume is a metric that determines how powerful a quantum computer is. It measures the length and complexity of quantum circuits, the building blocks of quantum applications. Just two months

ago, Honeywell similarly announced it had a quantum computer running client jobs with a Quantum Volume of 64. Honeywell reached the milestone with just a 6-qubit system.

IBM's previous Quantum Volume milestone, announced in January, was 32. The company said it reached a Quantum Volume of 64 through a series of new software and hardware techniques applied to a system already deployed within the IBM Q Network, a network of developers and industry professionals designed to collectively advance quantum computing.

More specifically, IBM said it achieved its improved results with a set of techniques that leveraged hardware to optimally run the quantum volume circuits. The methods should improve any quantum circuit run on any IBM Quantum system, the company said. They'll be available in upcoming releases to the IBM Cloud software services, as well as the cross-platform open source software development kit (SDK) Qiskit.

"IBM's full-stack approach gives a unique avenue to develop hardware-aware applications, algorithms and circuits, all running on the most extensive and powerful quantum hardware fleet in the industry," Jay Gambetta, IBM Fellow and VP of IBM Quantum, said in a statement.

IBM has made 28 quantum computers available on the IBM Cloud over the last four years, with eight systems running a Quantum Volume of 32.

19 Aug 2020

23 India is Amid a Quantum Boom

by Ryan F. Mandelbaum

https://medium.com/qiskit/india-is-amid-a-quantum-boom-7ab80870dd0d

Qiskit events draw students, researchers, and educators from around the world – but according to our data, interest is spiking in India, both in how users are engaging with the Qiskit open source community and in how often they're running IBM Quantum hardware.

Scientists in India have already started to undertake large-scale quantum projects. Three years ago, researchers began the country's first satellite-based quantum communication experiment – the Quantum Experiments using Satellite Technology, or QuEST project. Another team has been building an advanced new quantum computer. And earlier this year, India gave quantum technology a 80 billion rupee ($1.07 billion) boost as part of its National Mission on Quantum Technologies and Applications, coordinating stakeholders from across industry, research, and government to spur development in quantum computing, cryptography, communications, and materials science. These efforts are set to have a global impact, while a quantum community is coalescing around newly available opportunities in the field.

"It's a great time to be doing quantum physics because the government is serious about it, the people are serious about it, and we're all excited about what this technology can do for India," said Rishab Chatterjee, a graduate student from the Raman Research Institute in Bangalore, India.

An Advanced New QKD Simulator

A pioneering team led by Dr. Urbasi Sinha at the Raman Research Institute in Bangalore is poised to make a global impact when it comes to quantum key distribution (QKD). The researchers couldn't

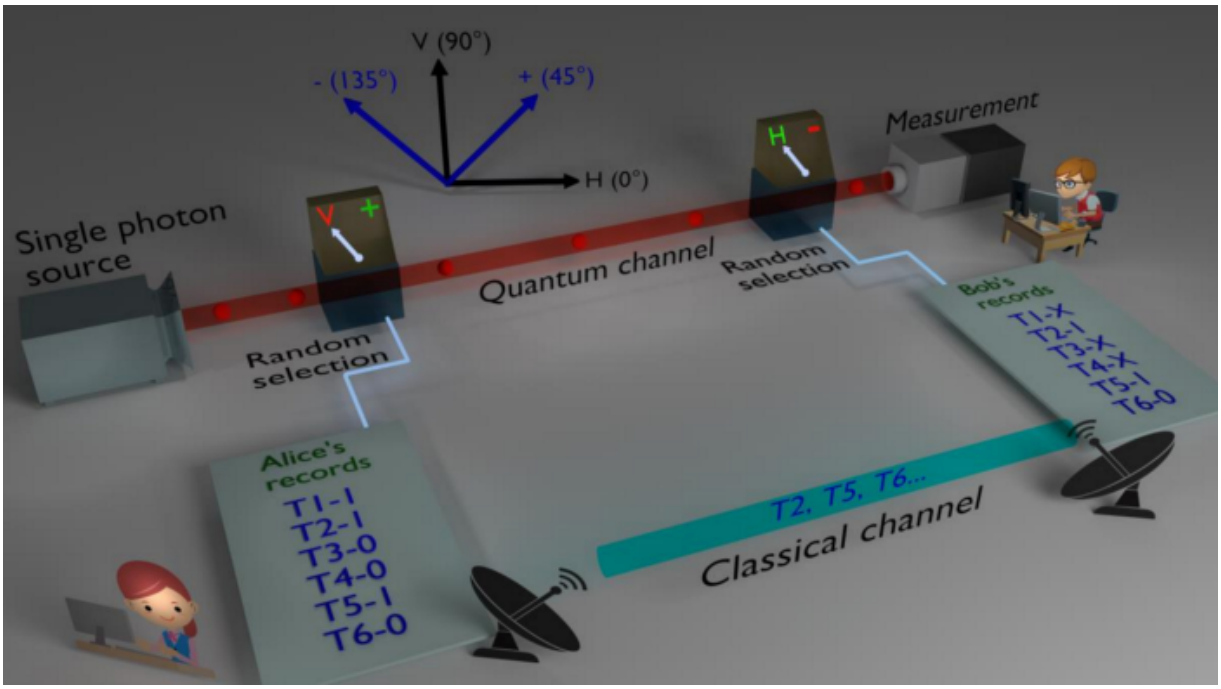


Figure 1: An explanation of the B92 protocol

find a public domain simulation software that took into account realistic imperfections of an experimental setup– so they developed a toolkit themselves and named it **qkdSim**. The team based primarily at the Raman Research Institute in Bangalore, India went on to successfully simulate an experimental setup of a QKD protocol and verify it with an actual demonstration of the protocol in free space. The experiment is a milestone for India as one of the country's first published free-space quantum key distribution experiments, and a foundational experiment as the country grows its QKD capabilities.

"QKD is already being used and deployed in other countries, but not as much so in India," said study author and RRI professor Urbasi Sinha. "Now that QKD is entering the commercial domain, such a simulation toolkit is of primary importance, not just here, but everywhere in the world – if you can simulate the whole system with almost every error you can think of, then you can ensure your resources won't go to waste. Now we'll be able to spend our money more wisely, and also have more confidence plus a benchmark for future QKD experiments."

Quantum key distribution is a form of cryptography where the laws of quantum mechanics create a system such that it's clear when someone is eavesdropping. There are plenty of other QKD simulators for educational and theoretical purposes, but few that actually take experimental components into account. Sinha and her team realized that as QKD matures, scientists and businesses will want to predict experimental results, including the errors, in order to build cheaper cryptography systems. Such a simulation must move beyond making theoretical predictions and incorporate how experimental components might alter important metrics like how quickly the key is generated or the error rate. QkdSim takes experimental parameters as its inputs, such as which QKD protocol to use, the experimental setup and components, the physical processes involved, and how long the protocol will run for.

The team carried out and simulated the B92 protocol, devised by IBM's Charles Bennett in 1992, which relies on Heisenberg's Uncertainty principle to generate quantum keys. In quantum systems, measuring in one basis randomizes the measurement in an orthogonal basis, as with a qubit's 0/1 and +/- bases or

a photon's horizontal/vertical and ±45 degree bases. For this protocol, Alice sends a random sequence of either vertically or +45 degree-polarized photons, which represent 0 and 1 respectively, and then Bob randomly chooses whether he'd like to measure those photons in the horizontal-vertical or the ±45 degree basis. If Alice sends a vertically polarized photon and Bob measures in the horizontal/vertical basis, then he'll always observe a vertically polarized photon, but if he measures in the ±45 degree basis, then he'll randomly observe a + or -45 degree-polarized photon. The converse occurs if Alice sends a +45 degree-polarized photon, with Bob either correctly measuring the +45 degree-polarized photon or incorrectly measuring horizontally and vertically polarized photons at random. Whenever Bob uses the wrong basis and measures a value that Alice didn't send, he knows for sure that the photon was sent in the other basis, and therefore knows its exact value since Alice only sent vertical and +45 degree-polarized photons. Bob publicly announces which photons were horizontally or -45 degree-polarized without announcing how he measured them, and then both Alice and Bob discard everything except the known photons. If the measured error is below a certain threshold, then the two can use the resulting bit string to send encrypted messages using the public and private information that the protocol generated. If the error is above the threshold, then an eavesdropper might be listening in.

The team demonstrated the protocol by sending single photons via an optical process called spontaneous parametric down-conversion, where a non-linear crystal generates a pair of low-energy photons from a high-energy pump photon. A set of filters removes all of the beam photons except for the generated pair, which then pass through a beam splitter. One photon goes to Bob, while Alice detects the other and records its time stamp; if Alice receives a horizontally polarized photon, then she knows she sent Bob a vertically polarized photon. The sent photon goes through another beam splitter that randomly selects between either the vertical and +45 degree states. Two meters away, Bob has his own beam splitter, set of optics, and a pair of detectors, which measure the incoming photons, perform the discarding step, and record timestamps. Bob only shares his timestamp data and not which detector it came from with Alice, then she returns his timestamp data discarding the events she didn't detect herself. This generates the same key for both of them. When the team ran the simulation given their own experimental components, run time, and the distance between Alice and Bob, the simulated results matched the experimental results almost exactly.

QkdSim is still in its first iteration of development, and will be including further non-idealities and imperfections in the subsequent versions, enabling a closer match with the experimental results. The team will also be incorporating a graphical user interface to the simulator. In the future, it may also be interesting to see if certain quantum resources required by QKD, like entanglement, could benefit from simulations on quantum hardware like IBM's quantum computers.

Ultimately, simulators like these will be of great value given how they can reduce the development costs of QKD, said Arash Atashpendar, RDI Manager at itrust consulting not involved in the study. This is especially true in more expensive QKD implementations, like satellite-based QKD.

A Three-In-One Quantum Architecture

When Rajamani "Vijay" Vijayaraghavan started his Ph.D in the United States under pioneering quantum computing expert Michel Devoret, he knew that he wanted to return to India in order to do cutting-edge research in his home country. But India was traditionally stronger in quantum theory, and funding for larger experimental endeavors was hard to come by, he said. Vijay focused on small, interesting problems relating to quantum computing components, like, microwave electronics, or developing different ways to think about superconducting qubits.

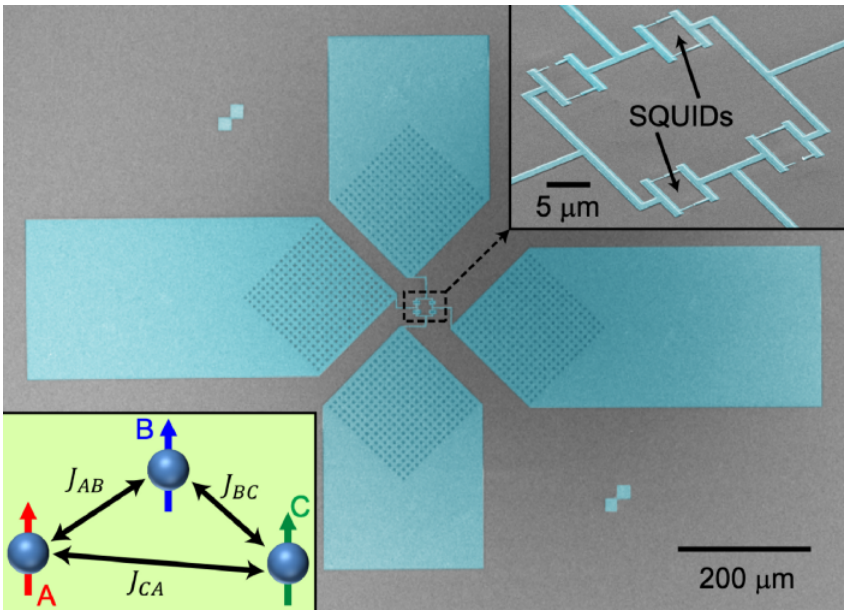


Figure 2: False-color scanning electron microscope image of a trimon system, with an inset depicting the beavior of the qubits.

In the past three years, his team has completely reoriented itself. “I did not anticipate that both the interest and support would accelerate to the level that it’s headed right now,” he said. The team is still looking at these interesting problems, but has now expanded its goals.

Vijay’s team is working on building a superconducting quantum computer based on “trimons,” rather than transmons. Transmon qubits, like those that form the basis of IBM’s quantum computers, consist of a circuit in superconducting wire where the electronic signal oscillates between a capacitor and a junction in the wire called a Josephson junction. The zero-point energy and the first mode represent the 0 and 1 qubit states, and the Josephson junction’s properties ensure that a different amount of energy is required to send the qubit from the 0 to 1 and from the 1 to 2 modes so it doesn’t accidentally oscillate in the higher modes during the calculation. Each trimon is instead a quantum circuit composed of four Josephson junctions and six capacitors that acts like three coupled transmons with its own system of modes in a three-qubit Hilbert space.

Trimons have some strengths and weaknesses versus transmons. Three-qubit gates are much easier to perform on trimon systems, and they present a different and potentially simpler way to implement some quantum algorithms, such as the Bernstein-Vazirani algorithm and Grover’s algorithm. At the same time, one- and two-qubit gates become more complicated on trimon systems.

As interest in quantum computing surges in India, and with support on the way from the National Mission, Vijay’s team is collaborating on projects with other groups, such as India’s Defense Research and Development Organization as well as Tata Consultancy Services, all while working to scale up their quantum device. They’re also working with IBM devices to benchmark their own trimon qubits, and hope to one day put a small quantum processor on the cloud that researchers can access via Qiskit. The main challenges in scaling up the system aren’t only the technical – it will also require attracting, training, and maintaining talent both from India and abroad, Vijay said.

Vijay pointed out that India isn’t building its quantum ecosystem on as old a foundation of experimental

research as universities in the United States and Europe. But, while it might seem to some like India is "late," there are still plenty of research breakthroughs necessary in the field. "A critical breakthrough today could change the course of the technology and happen anywhere in the world," he said. "Why not India?"

Building a Quantum Computing Community in India

As quantum computing interest grows in India, so too does the community around it. Community is crucial for growing and maintaining such an interdisciplinary field. "When I first got interested in quantum computing, there was a dearth of knowledge on how one could contribute to the field" said Rana Prathap Simh Mukthavaram, Co-op at IBM Quantum and Qiskit. "However, by meeting people and participating in competitions, I realized that there was a place for pretty much everyone who's interested."

Students, researchers, and scientists have formed clubs and organizations such as the non-profit organization **IndiQ**. Rahul Pratap Singh, Rana Prathap Simh Mukthavaram, Samanvay Sharma and Frederik Hardervig founded IndiQ with the help of Qiskit Advocate Junye Huang after Qiskit Camp Asia 2019. The group organizes events and meet-ups on quantum education and is now working to create awareness on quantum science and technology. IndiQ has already hosted a game jam, as well as meetups in Hyderabad, Delhi and Bangalore.

Qiskit has also hosted and will continue hosting events tailored to quantum researchers in India. On July 27, we held a meetup for professors in India to learn about Qiskit and network with one another. In early September, we'll be hosting the Qiskit Challenge India, a two-week-long quantum machine learning challenge exclusive to India where contestants will first be provided with learning material and exercises to strengthen their quantum computing knowledge before tackling a quantum classification problem.

Quantum computing interest in India isn't just coming from the top down – we've already noticed spikes in engagement on social media, plus thousands of signups in just the past few months for IBM's Quantum Experience as well as Qiskit. We just concluded our Qiskit Global Summer School, and students from India formed the largest group of attendees from any country aside from the United States. As a result of the summer school, QGSS participants interested in continuing to build a quantum community coalesced into a Discord server now managed by IndiQ.

As interest quantum computing expands around the globe, we're excited to see what people can do with Qiskit, and more importantly, the kinds of national and international communities that form as we build this field together. Qiskit

24 AI automatic tuning delivers step forward in quantum computing

by University of Oxford

https://techxplore.com/news/2020-08-ai-automatic-tuning-quantum.html

Researchers at Oxford University, in collaboration with DeepMind, University of Basel and Lancaster University, have created a machine learning algorithm that interfaces with a quantum device and 'tunes' it faster than human experts, without any human input. They are dubbing it "Minecraft explorer for quantum devices."

Classical computers are composed of billions of transistors, which together can perform complex calculations. Small imperfections in these transistors arise during manufacturing, but do not usually affect

the operation of the computer. However, in a quantum computer similar imperfections can strongly affect its behavior.

In prototype semiconductor quantum computers, the standard way to correct these imperfections is by adjusting input voltages to cancel them out. This process is known as tuning. However, identifying the right combination of voltage adjustments needs a lot of time even for a single quantum device. This makes it virtually impossible for the billions of devices required to build a useful general-purpose quantum computer.

Today in Nature Communications the scientists describe a machine learning algorithm that solves this problem. By tuning away the differences between quantum devices, they hope to make large quantum circuits feasible and unleash the potential of quantum technologies in fields ranging from medicine to cryptography.

Lead author Dr. Natalia Ares, from Oxford University's Department of Materials, says, "The difficulty in tuning has so far been a major hindrance for building large quantum circuits, since this task quickly becomes intractable. We have demonstrated that the tuning of our quantum devices can be done fully automatically using machine learning. This demonstration shows a promising route towards the scalability of quantum processors."

The scientists' machine learning algorithm takes a similar approach to a player of Minecraft. In this game, often the player is in a dark cave and has to find ore. They can use torches to illuminate parts of the cave, and once some ore is found, the expectation is that more might be found nearby. However, it is sometimes worth exploring other parts of the cave where more ore could be found. This is a trade-off between exploration and exploitation. In this case, the machine has to find the right operating conditions for the quantum device (ore) and with that aim it explores a dark cave (the space of parameters defined by the voltages). Once good operating conditions have been found, the exploitation-exploration trade-off comes to play. The torches are measurements of the quantum device, which are expensive and therefore scarce, so are a resource to be used wisely.

Dr. Ares says, "We were surprised that the machine was better than humans in the laboratory, we have been learning how to efficiently tune quantum devices for years. For humans, it requires training, knowledge about the physics of the device and a bit of intuition!"

"Our ultimate goal is to fully automate the control of large quantum circuits, opening the path to completely new technologies which harness the particularities of quantum physics."

Co-author, Dr. Edward Laird of Lancaster University, says "When I was a Ph.D. student in the 2000s (in the same lab with Dominik Zumbühl, who is one of the collaborators on this project from University of Basel), I would often spend weeks tuning one prototype qubit by hand. We all knew that we would need to automate the task one day, but I had no idea how that could work. Thanks to machine learning, we can now see a way to do it. I hope soon we will be able to use our approach to completely tune a small-scale quantum computer."

25 Tata Teleservices, FirstWave to launch cybersecurity solutions

by Muntazir Abbas

https://telecom.economictimes.indiatimes.com/news/tata-teleservices-firstwave-to-launch-cybersecurity-solutions/77615793

Tata Teleservices and Australian cybersecurity company FirstWave will be collaborating to bring a complete range of platform-based security solutions for enterprise customers in India.

"Our partnership with FirstWave will bring their comprehensive portfolio of next-generation platform-based security solutions to our enterprise customers in India," Sai Pratyush, Group Product Head – IoT and Cloud at Tata Teleservices told ET Telecom.

The two companies are expected to enter into partnership later this week.

Mumbai-based company is planning to leverage FirstWave's Software as a Service (SaaS) orchestration technology platform, cloud content security provider (CCSP) to launch multiple security services incorporating Web, email, next-generation firewall, endpoint and multi-factor authentication (MFA).

The security platform, according to Pratyush, will enable telco's customers to easily access comprehensive cybersecurity solutions that could be rapidly deployed on affordable subscription prices.

In February this year, the Department of Telecom (DoT) approved Tata Teleservices consumer mobile business with Sunil Mittal-driven Bharti Airtel while the company continues to operate its business services, and have many big-ticket customers.

Tata Tele Business Services, a part of the Tata group companies has a fibre optic network spread of nearly 150,000 kilometers and operates in close to 70 large cities.

"These solutions will secure our customers using public and private cloud applications while delivering operational efficiencies and reducing their overall security management cost due to multi-tenanted architecture," the top executive said.

"We have a strong customer base amongst enterprises and startups across sectors such as BFSI, IT/ITeS, manufacturing, fintech, healthcare, logistics and e-commerce sectors," he added.

Pratyush believes that investing in cybersecurity is no longer an option, but it has become a necessity since the COVID-19 pandemic has presented a once-in-a-lifetime opportunity for hackers and online scammers, with an increased number of cyberattacks currently.

Tata Tele Business Services has a network of more than 1,500 channel partners while the new portfolio would be available through the company's digital platform.

18 Aug 2020

26 How Intel will keep Moore's Law cranking for years to come

by Stephen Shankland

https://www.cnet.com/news/how-intel-will-keep-moores-law-cranking-for-years-to-come/

Moore's Law, the observation that the number of transistors on a computer chip doubles every 24 months, has taken a beating as progress miniaturizing circuitry falters. But chip giant Intel has plotted a course to keep the idea alive with a plan to pack 50 times as many transistors onto processors than is possible today.

The progress of Moore's Law, named after Intel co-founder Gordon Moore, has spread chips from expensive mainframes in the 1960s to personal computers in the 1980s and now to smartphones, watches, cars, TVs, washing machines and just about anything with electrical power.

Moore's Law has worked by shrinking transistors, the data-processing elements on a chip. Intel plans to keep shrinking them, but also to increase density by stacking chips into multilayer packages.

"We firmly believe there is a lot more transistor density to come," said Intel Chief Architect Raja Koduri, in a speech Monday for the Hot Chips conference for cutting-edge processor revelations. "The vision will play out over time – maybe a decade or more – but it will play out."

Koduri's optimism mirrored the excitement of many other companies at Hot Chips, an engineering conference where researchers detail progress. AMD, Nvidia, Google, Microsoft, IBM and a gaggle of startups showed ways they're advancing both general-purpose chips and those dedicated to tasks such as artificial intelligence, graphics and networking.

How Intel expects to deliver chip progress

Koduri described several steps to cram more transistors into a chip than possible with 10nm chips like its **Tiger Lake** processor arriving in laptops this fall. First will come the most traditional approach, shrinking transistors and squeezing them closer together. That'll triple the transistor density, Koduri predicted.

Next up are new transistor designs that continue the current transformation of transistors from flat circuitry elements into 3D structures. These steps, called nanowires and stacked nanowires, should quadruple density.

Then come packaging innovations, with chips stacked into a layer cake of processor elements. That should quadruple density again. The total math brings density up by about a factor of 50.

Years of Intel difficulties

Intel's optimism contrasts with difficult times keeping Moore's Law ticking.

Intel, once the unquestioned leader in chip manufacturing, has struggled in recent years. Its move from a manufacturing process with transistor features measuring 14 nanometers to later 10nm took five years instead of two. A nanometer is a billionth of a meter, and with circuitry elements 14nm wide, Intel can pack about 7,000 across the width of a human hair.

Next, Intel delayed its move from 10nm to 7nm manufacturing by six months, and Apple is dumping Intel chips from its Macs. To help adjust, Intel has adopted a more flexible design process that lets it rely more on other chipmakers like its top rival, Taiwan Semiconductor Manufacturing Corp.

Moore's Law, but at what cost?

TSMC, which moved to 7nm manufacturing about two years ago and makes Apple's iPhone chips, last year declared "Moore's Law is well and alive." But unlike in the past, Moore's Law steps now impose new costs for companies that want to employ the most advanced manufacturing processes.

Microsoft's Xbox One in 2013, Xbox One X in 2017, and Xbox Series X coming this year all have chips about the same size, which in the past would have meant that the chips cost about the same price. Now, though, "it's significantly more expensive for the newest one," said Microsoft chip designer Jeff Andrews.

Another challenge besides cost is that new chips often only accelerate specific computing operations. That's useful for tasks like artificial intelligence and graphics, but it makes life harder for software programmers who have to reckon with processors that work in different ways.

Intel is trying to bridge this chip divide with a new software layer it calls oneAPI. It's a notable move: Intel is a hardware specialist, but it's embracing software as an essential step in making its chips useful.

"Increasingly, hardware architecture teams need to be comprised of software experts," Koduri said.

New chip ideas

At Hot Chips, processor makers also detailed a host of innovations. Among the biggest:

- Intel's **Tiger Lake** processor uses a new incarnation of power-saving technology called DVFS, or dynamic voltage and frequency scaling. Different parts of the chip can run faster for high-priority tasks or slower to save power. Intel now juggles the priorities between its multiple processor cores, the memory system and the communication fabric that connects it all together.
- AMD's competing **Ryzen 4000 series chips**, code-named Renoir and arriving now in PCs, are the first chips with eight processing cores for super-thin laptops. AMD had initially planned a six-core design but realized a careful design could accommodate eight for better performance on tasks like video and photo editing, said architect Sonu Arora. They use half the power for a given performance level as their predecessors.
- IBM's **Power10 processors**, which have 18 billion transistors and are due in massive Unix servers arriving next year, can be ganged together into a single powerful server with as many as 240 processing cores. In addition, a "pod" of interlinked servers can share as much as 2 petabytes of memory. That's useful for massive business computing challenges like data mining and managing inventory databases.
- Startup Lightmatter unveiled its **Mars chip** for accelerating AI work like image recognition. It marries about a billion conventional transistors with tens of thousands of components that use light instead of electricity to transfer data and perform calculations. The idea behind this photonic technology is to cut power usage.

27 Excitons bound by photon exchange

https://www.swissquantumhub.com/excitons-bound-by-photon-exchange/

A team of researchers successfully created the first artificial atom using photons as threads to weave electrons together.

In contrast to interband exciton in undoped quantum wells, doped quantum wells do not display sharp resonances due to excitonic bound states. The effective Coulomb interaction between electrons and holes in these systems typically leads to only a depolarization shift of the single-electron intersubband transitions. Non-perturbative light-matter interaction in solid-state devices has been investigated as a pathway to tuning optoelectronic properties of materials.

A recent theoretical work predicted that when the doped quantum wells are embedded in a photonic cavity, emission-reabsorption processes of cavity photons can generate an effective attractive interaction that binds electrons and holes together, leading to the creation of an intraband bound exciton.

The scientists spectroscopically observed such a bound state as a discrete resonance that appeared below the ionization threshold only when the coupling between light and matter is increased above a critical value.

Their result has demonstrated that two charged particles can be bound by the exchange of transverse photons. Light-matter coupling can thus be used as a tool in quantum material engineering, tuning electronic properties of semiconductor heterostructures beyond those permitted by mere crystal structures, with direct applications to mid-infrared optoelectronics.

17 Aug 2020

28 A new mathematical tool to simulate quantum material's properties more quickly

by AMIT MALEWAR

https://www.techexplorist.com/new-mathematical-tool-simulate-quantum-materials-properties-quickly/34749/

Quantum Monte Carlo (QMC) methods are the gold standard for studying equilibrium properties of quantum many-body systems. However, in many unusual situations, QMC methods are faced with a significant problem, causing the severe limitation of an exponential increase in the runtime of the QMC algorithm.

The calculation of quantum material characteristics costs about one million hours of CPU on mainframe computers every day.

In a new study, a joint research group at Freie Universität Berlin and the Helmholtz-Zentrum Berlin (HZB, Germany) has demonstrated a systematic, generally applicable, and practically feasible methodology for easing the sign problem by efficiently computable basis changes and use it to assess the sign problem rigorously.

Dominik Hangleiter, the first author of the study, said, "We show that solid-state systems can be viewed from very different perspectives. The sign problem plays a different role in these different perspectives. It is then a matter of dealing with the solid-state system in such a way that the sign problem is minimized."

For basic strong state systems with spins, which structure what are known as Heisenberg ladders, this methodology has empowered the group to decrease the sign problem's computational time significantly. Be that as it may, the numerical tool can likewise be applied to more complex spin systems and promises quicker computation of their properties.

Prof. Jens Eisert, who heads the joint research group at Freie Universität Berlin and the HZB, said, "This provides us with a new method for accelerated development of materials with special spin properties. These materials could find application in future IT technologies for which data must be processed and stored with considerably less energy expenditure."

14 Aug 2020

29 Computer scientists set benchmarks to optimize quantum computer performance

by University of California

https://techxplore.com/news/2020-08-scientists-benchmarks-optimize-quantum.html

Two UCLA computer scientists have shown that existing compilers, which tell quantum computers how to use their circuits to execute quantum programs, inhibit the computers' ability to achieve optimal performance. Specifically, their research has revealed that improving quantum compilation design could help achieve computation speeds up to 45 times faster than currently demonstrated.

The computer scientists created a family of benchmark quantum circuits with known optimal depths or sizes. In computer design, the smaller the circuit depth, the faster a computation can be completed. Smaller circuits also imply more computation can be packed into the existing quantum computer. Quantum computer designers could use these benchmarks to improve design tools that could then find the best circuit design.

"We believe in the 'measure, then improve' methodology," said lead researcher Jason Cong, a Distinguished Chancellor's Professor of Computer Science at UCLA Samueli School of Engineering. "Now that we have revealed the large optimality gap, we are on the way to develop better quantum compilation tools, and we hope the entire quantum research community will as well."

Cong and graduate student Daniel (Bochen) Tan tested their benchmarks in four of the most used quantum compilation tools. A study detailing their research was published in IEEE Transactions on Computers, a peer-reviewed journal.

Tan and Cong have made the benchmarks, named QUEKO, open source and available on the software repository GitHub.

Quantum computers utilize quantum mechanics to perform a great deal of computations simultaneously, which has the potential to make them exponentially faster and more powerful than today's best supercomputers. But many issues need to be addressed before these devices can move out of the research lab.

For example, due to the sensitive nature of how quantum circuits work, tiny environmental changes, such as small temperature fluctuations, can interfere with quantum computation. When that happens, the quantum circuits are called decoherent – which is to say they have lost the information once encoded in them.

"If we can consistently halve the circuit depth by better layout synthesis, we effectively double the time it takes for a quantum device to become decoherent," Cong said.

"This compilation research could effectively extend that time, and it would be the equivalent to a huge advancement in experimental physics and electrical engineering," Cong added. So we expect these benchmarks to motivate both academia and the industry to develop better layout synthesis tools, which in turn will help drive advances in quantum computing."

Cong and his colleagues led a similar effort in the early 2000s to optimize integrated circuit design in classical computers. That research effectively pushed two generations of advances in computer processing speeds, using only optimized layout design, which shortened the distance between the transistors that comprise the circuit. This cost-efficient improvement was achieved without any other major investments in technological advances, such as physically shrinking the circuits themselves.

"Quantum processors in existence today are extremely limited by environmental interference, which puts severe restrictions on the length of computations that can be performed," said Mark Gyure, executive director of the UCLA Center for Quantum Science and Engineering, who was not involved in this study. "That's why the recent research results from Professor Cong's group are so important because they have shown that most implementations of quantum circuits to date are likely extremely inefficient and more

optimally compiled circuits could enable much longer algorithms to be executed. This could result in today's processors solving much more interesting problems than previously thought. That's an extremely important advance for the field and incredibly exciting."

13 Aug 2020

30 Amazon launches Braket quantum computing service in general availability

by Kyle Wiggers

https://venturebeat.com/2020/08/13/amazon-launches-braket-quantum-computing-service-in-general-availability/

Amazon today announced the general availability of Amazon Braket, a fully managed Amazon Web Services (AWS) product that provides a development environment for exploring and designing novel quantum algorithms. Customers can tap Braket – which launched in preview last December – to test and troubleshoot algorithms on simulated quantum computers running in the cloud to help verify their implementation. Users can then run those algorithms on quantum processors in systems from D-Wave, IonQ, and Rigetti.

In theory, quantum computing has the potential to solve problems beyond the reach of classical computers by harnessing the laws of quantum mechanics to build powerful information-processing tools. Scientific discoveries arising from quantum computing could transform energy storage, chemical engineering, drug discovery, financial portfolio optimization, machine learning, and more. But advances require in-house expertise, access to quantum hardware, or a combination of both. Amazon asserts that managed quantum infrastructure could help facilitate research and education in quantum technologies and accelerate breakthroughs.

Using Jupyter notebooks and existing AWS services, Braket users can assess present and forthcoming capabilities, including quantum annealing, ion trap devices, and superconducting chips. Amazon says partners were chosen "for their quantum technologies" and that customers and hardware providers can design quantum algorithms using the Braket developer toolkit. They can also access a library of prebuilt algorithms and execute either low-level quantum circuits or fully managed hybrid algorithms, as well as selecting between software simulators running in AWS Elastic Cloud Compute and quantum hardware.

In addition to running quantum algorithms, customers can use Braket to run hybrid algorithms, which combine quantum and classical computing systems to overcome limitations inherent in today's quantum technology. They're also given access to Amazon's Quantum Solutions Lab, which aims to connect users with quantum computing experts – including from 1Qbit, Rahko, Rigetti, QC Ware, QSimulate, Xanadu, and Zapata – to identify ways to apply quantum computing inside their organizations.

Amazon says **Volkswagen** has tested Braket to gain an "in-depth understanding of the meaningful use of quantum computing in a corporate environment." Other early adopters include multinational power company **Enel**, biotechnology organization **Amgen**, the University of Waterloo's **Institute for Quantum Computing**, quantum machine learning startup **Rahko, Qu & Co**, and the **Fidelity Center for Applied Technology**.

Amazon Braket is available today in US East (N. Virginia), US West (N. California), and US West (Oregon) AWS Regions, with more regions planned.

Braket competes with Microsoft's Azure Quantum, a service that offers select partners access to three prototype quantum computers from IonQ, Honeywell, and QCI. But Azure Quantum is still in preview. And other rival offerings from Google and IBM only deliver compute from single, proprietary quantum processors and machines.

In a sign of its commitment to quantum computing research, Amazon unveiled the AWS Center for Quantum Computing last December. The Caltech-based laboratory aims to "boost innovation in science and industry" by connecting Amazon researchers and engineers with academic institutions to develop more powerful quantum computing hardware and identify novel quantum applications.

12 Aug 2020

31 DARPA Investing in Encryption to Secure "Internet of Things"

by Chris Cornillie

https://about.bgov.com/news/darpa-investing-in-encryption-to-secure-internet-of-things/

The Defense Advanced Research Projects Agency (DARPA) is seeking information on ways to secure billions of internet-connected devices against futuristic code-breaking tools, according to an Aug. 11 sources-sought notice.

DARPA officials envision a not-too-distant future in which billions, perhaps trillions, of small electronic devices – security cameras, drones, self-driving vehicles, and even household appliances like toasters – are connected over 5G wireless networks. The connectivity of devices forms the basis of what's known as the "Internet of Things," or the IoT. Because these devices are simple in terms of built-in computing power, robust encryption is often an afterthought.

To make matters worse, quantum computers will render most forms of conventional cryptography now used to secure data obsolete over the next 15 years, according to experts at the National Institute of Standards and Technology (NIST). This raises the risk that billions of devices may be at risk of cyberattack.

"Revolutionary security technologies are needed for IoT devices," according to the Aug. 11 notice.

DARPA plans to launch a new Small Business Innovation Research and Small Business Technology Transfer (SBIR/STTR) program called Cryptography for Hyper-scale Architectures in a Robust Internet of Things (CHARIOT). The program will focus on prototyping encryption technologies that are "fast, efficient, and quantum-resistant on even the cheapest devices," according to the document. DARPA officials are especially interested in applications relevant to wearable devices and vehicle-embedded systems.

DARPA officials are accepting proposals for Direct to Phase 2 funding under the SBIR/STTR program, allowing the agency to fast-track investment in promising commercial prototypes. The agency may issue multiple awards, each with a two-year base period of performance and maximum value of $1.5 million, and a 12-month option period worth up to $500,000. The deadline to submit proposals is Sept. 29.

DARPA requested $1.1 billion in unclassified funding for 70 projects related to cryptography or cybersecurity in its fiscal 2021 Research, Development, Test & Evaluation (RDT&E) budget, according to Bloomberg Government's RDT&E Dashboard. It also requested $171 million for nine projects related to quantum information sciences. DARPA's total unclassified RDT&E budget request for fiscal 2021 was $3.6 billion.

32 Quantum researchers create an error-correcting cat

by Yale University

https://www.sciencedaily.com/releases/2020/08/200812144017.htm#:~:text=Yale%20physicists%20have%20developed%20an,errors%20in%20a%20quantum%20computation.

Yale physicists have developed an error-correcting cat – a new device that combines the Schrödinger's cat concept of superposition (a physical system existing in two states at once) with the ability to fix some of the trickiest errors in a quantum computation.

It is Yale's latest breakthrough in the effort to master and manipulate the physics necessary for a useful quantum computer: correcting the stream of errors that crop up among fragile bits of quantum information, called qubits, while performing a task.

A new study reporting on the discovery appears in the journal Nature. The senior author is Michel Devoret, Yale's F.W. Beinecke Professor of Applied Physics and Physics. The study's co-first authors are Alexander Grimm, a former postdoctoral associate in Devoret's lab who is now a tenure-track scientist at the Paul Scherrer Institute in Switzerland, and Nicholas Frattini, a graduate student in Devoret's lab.

Quantum computers have the potential to transform an array of industries, from pharmaceuticals to financial services, by enabling calculations that are orders of magnitude faster than today's supercomputers.

Yale – led by Devoret, Robert Schoelkopf, and Steven Girvin – continues to build upon two decades of groundbreaking quantum research. Yale's approach to building a quantum computer is called "circuit QED" and employs particles of microwave light (photons) in a superconducting microwave resonator.

In a traditional computer, information is encoded as either 0 or 1. The only errors that crop up during calculations are "bit-flips," when a bit of information accidentally flips from 0 to 1 or vice versa. The way to correct it is by building in redundancy: using three "physical" bits of information to ensure one "effective" – or accurate – bit.

In contrast, quantum information bits – qubits – are subject to both bit-flips and "phase-flips," in which a qubit randomly flips between quantum superpositions (when two opposite states exist simultaneously).

Until now, quantum researchers have tried to fix errors by adding greater redundancy, requiring an abundance of physical qubits for each effective qubit.

Enter the cat qubit – named for Schrödinger's cat, the famous paradox used to illustrate the concept of superposition.

The idea is that a cat is placed in a sealed box with a radioactive source and a poison that will be triggered if an atom of the radioactive substance decays. The superposition theory of quantum physics suggests that until someone opens the box, the cat is both alive and dead, a superposition of states. Opening the box to observe the cat causes it to abruptly change its quantum state randomly, forcing it to be either alive or dead.

"Our work flows from a new idea. Why not use a clever way to encode information in a single physical system so that one type of error is directly suppressed?" Devoret asked.

Unlike the multiple physical qubits needed to maintain one effective qubit, a single cat qubit can prevent phase flips all by itself. The cat qubit encodes an effective qubit into superpositions of two states within a single electronic circuit – in this case a superconducting microwave resonator whose oscillations correspond to the two states of the cat qubit.

"We achieve all of this by applying microwave frequency signals to a device that is not significantly more complicated than a traditional superconducting qubit," Grimm said.

The researchers said they are able to change their cat qubit from any one of its superposition states to any other superposition state, on command. In addition, the researchers developed a new way of reading out – or identifying – the information encoded into the qubit.

"This makes the system we have developed a versatile new element that will hopefully find its use in many aspects of quantum computation with superconducting circuits," Devoret said.

11 Aug 2020

33 evolutionQ Awarded Contribution from Canada Space Agency for Quantum Key Distribution Network R&D

https://www.hpcwire.com/off-the-wire/evolutionq-awarded-contribution-from-canada-space-agency-for-quantum-key-distribution-network-rd/#:~:text=KITCHENER%2C%20Ontario%2C%20Aug.%2011,Key%20Distribution%20(QKD)%20networks.

evolutionQ was awarded a Space Technology Development Program (STDP) contribution by the CSA to develop solutions to advance satellite-based secure quantum communication services and tools to address challenges related to satellite-based Quantum Key Distribution (QKD) networks.

Cryptography underpins the secure communications required for the digital, network-based social and financial interactions that are at the heart of modern society and the economy, including banking, the sharing of confidential healthcare data, and the exchange of sensitive information between governmental institutions. However, rapid advancements in quantum computing threaten current encryption methods because quantum computers, when built, will be able to break commonly used cybersecurity systems. It is important to develop tools, like QKD, that will be resistant to such quantum threats.

QKD technologies leverage the fundamental laws of quantum physics to distribute confidential cryptographic keys between two users while detecting the attempts of malicious third-parties to intercept such keys. Unfortunately, typical terrestrial methods to establish such direct secure connection between locations are limited to relatively short distances, of the order of at most 200 km. This is clearly a challenge for a country as vast as Canada. Satellite-based QKD will enable secure, reliable, and economical key-sharing across Canada.

"A powerful quantum computer has the power to decimate today's cryptography. As key quantum computing milestones are achieved, the need for quantum-safe solutions intensifies," said Dr. Michele Mosca, President and CEO of evolutionQ. "Robust cryptography is absolutely necessary for our safety and the proper functioning of our digital economy. We must adopt quantum-safe solutions to secure and safeguard our critical infrastructures, financial services and intellectual property."

"Quantum Key Distribution is an important tool in addressing the quantum threat. QKD uses the fundamental laws of physics to protect information shared between two parties." CTO of evolutionQ, Dr. Norbert Lütkenhaus remarked. "Satellite-based QKD is essential for a vast country like Canada and will help secure communications from coast to coast. evolutionQ is poised to utilize its expertise and develop solutions to help establish satellite QKD, and to integrate it with existing terrestrial solutions."

evolutionQ will develop tools to address the challenges unique to satellite-based QKD. This will be accomplished by modeling the role and performance of QKD satellites, and by designing optimization

algorithms to integrate QKD satellites with terrestrial networks. The software solutions will be designed to be integrated with existing and planned satellite hardware. The project is expected to last 24 months.

The initiative will also help Canada safeguard sovereignty in the quantum age and strengthen Canadian leadership in the space and quantum sectors. The initiative aligns with the new Space Strategy for Canada, the safety and security principle in Canada's Digital Charter and the Government of Canada's Innovations and Skills Plan.

34 Honeywell Wants To Show What Quantum Computing Can Do For The World

by Gil Press

https://www.forbes.com/sites/gilpress/2020/08/11/honeywell-wants-to-show-what-quantum-computing-can-do-for-the-world/#1f9bf1172916

The race for quantum supremacy heated up in June, when Honeywell brought to market the "world's highest performing quantum computer." Honeywell claims it is more accurate (i.e., performs with less errors) than competing systems and that its performance will increase by an order of magnitude each year for the next five years.

"The beauty of quantum computing," says Tony Uttley, President of Honeywell Quantum Solutions, "is that once you reach a certain level of accuracy, every time you add a qubit you double the computational capacity. So as the quantum computer scales exponentially, you can scale your problem set exponentially."

Uttley sees three distinct eras in the evolution of quantum computing. Today, we are in the emergent era – "you can start to prove what kind of things work, what kind of algorithms show the most promise." For example, the Future Lab for Applied Research and Engineering (FLARE) group of JPMorgan Chase published a paper in June summarizing the results of running on the Honeywell quantum computer complex mathematical calculations used in financial trading applications.

The next era Uttley calls classically impractical, running computations on a quantum computer that typically are not run on today's ("classical") computers because they take too long, consume too much power, and cost too much. "Crossing the threshold from emergent to classically impractical is not very far away," he asserts, probably sometime in the next 18 to 24 months. "This is when you build the trust with the organizations you work with that the answer that is coming from your quantum computer is the correct one," says Uttley.

The companies that understand the potential impact of quantum computing on their industries, are already looking at what it would take to introduce this new computing capability into their existing processes and what they need to adjust or develop from scratch, according to Uttley. These companies will be ready for the shift from "emergent" to "classically impractical" which is going to be "a binary moment," and they will be able "to take advantage of it immediately."

The last stage of the quantum evolution will be classically impossible – "you couldn't in the timeframe of the universe do this computation on a classical best-performing supercomputer that you can on a quantum computer," says Uttley. He mentions quantum chemistry, machine learning, optimization challenges (warehouse routing, aircraft maintenance) as applications that will benefit from quantum computing. But "what shows the most promise right now are hybrid [resources] – "you do just one thing, very efficiently, on a quantum computer," and run the other parts of the algorithm or calculation on a classical computer.

Uttley predicts that "for the foreseeable future we will see co-processing," combining the power of today's computers with the power of emerging quantum computing solutions.

"You want to use a quantum computer for the more probabilistic parts [of the algorithm] and a classical computer for the more mundane calculations – that might reduce the number of qbits needed," explains Gavin Towler, vice president and chief technology officer of Honeywell Performance Materials Technologies. Towler leads R&D activities for three of Honeywell's businesses: Advanced Materials (e.g., refrigerants), UOP (equipment and services for the oil and gas sector), and Process Automation (automation, control systems, software, for all the process industries). As such, he is the poster boy for a quantum computing lead-user.

"In the space of materials discovery, quantum computing is going to be critical. That's not a might or could be. It is going to be the way people do molecular discovery," says Towler. Molecular simulation is used in the design of new molecules, requiring the designer to understand quantum effects. "These are intrinsically probabilistic as are quantum computers," Towler explains.

An example he provides is a refrigerant Honeywell produces that is used in automotive air conditioning, supermarkets refrigeration, and homes. As the chlorinated molecules in the refrigerants were causing the hole in the Ozone layer, they were replaced by HFCs which later tuned out to be very potent greenhouse gasses. Honeywell already found a suitable replacement for the refrigerant used in automotive air conditioning, but is searching for similar solutions for other refrigeration applications. Synthesizing in the lab molecules that will prove to have no effect on the Ozone layer or global warming and will not be toxic or flammable is costly. Computer simulation replaces lab work "but ideally, you want to have computer models that will screen things out to identify leads much faster," says Towler.

This is where the speed of a quantum computer will make a difference, starting with simple molecules like the ones found in refrigerants or in solvents that are used to remove CO2 from processes prevalent in the oil and gas industry. "These are relatively simple molecules, with 10-20 atoms, amenable to be modeled with [today's] quantum computers," says Towler. In the future, he expects more powerful quantum computers to assist in developing vaccines and finding new drugs, polymers, biodegradable plastics, "things that contain hundred and thousands of atoms."

There are three ways by which Towler's counterparts in other companies, the lead-users who are interested in experimenting with quantum computing, can currently access Honeywell's solution: Run their program directly on Honeywell's quantum computer; through Microsoft Azure Quantum services; and working with two startups that Honeywell has invested in, Cambridge Quantum Computing (CQC) and Zapata Computing, both assisting in turning business challenges into quantum computing and hybrid computing algorithms.

Honeywell brings to the quantum computing emerging market a variety of skills in multiple disciplines, with its decades-long experience with precision control systems possibly the most important one. "Any at-scale quantum computer becomes a controls problem," says Uttley, "and we have experience in some of the most complex systems integration problems in the world." These past experiences have prepared Honeywell "to show what quantum computing can do for the world" and to rapidly scale-up its solution. "We've built a big auditorium but we are filling out just a few seats right now and we have lots more seats to fill," Uttley sums up this point in time in Honeywell's journey to quantum supremacy.

35 ETSI releases migration strategies and recommendations for Quantum-Safe schemes

by Sophia Antipolis

https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes?jjj=1597327943624

The ETSI Quantum-Safe Cryptography (QSC) working group is pleased to announce the release of Technical Report TR 103 619 defining migration strategies and recommendations for Quantum-Safe schemes, and enhancing cryptography awareness across all business sectors.

The threat of quantum computing to asymmetric cryptography has been extensively reported in ETSI's work and elsewhere, and has been recognized as an existential threat to the many business sectors that rely on asymmetric cryptography for their day-to-day existence. However, recognizing the threat is not sufficient, nor is knowing that a quantum-safe cryptographic algorithm exists to enable encrypted assets in a business to be protected. The entire business must now be ready to migrate to a new Fully Quantum-Safe Cryptographic State (FQSCS). In anticipation of this, ETSI has developed a new technical report defining a framework of actions that an organization should take to enable migration to a Fully Quantum-Safe Cryptographic State.

"*What we lay out in the migration Report is getting the role of cryptography and the depth of its integration in a business better understood. We need to increase cryptography awareness so that people send out encrypted data keeping in mind that it may be commercially sensitive years later when attacks are possible. This helps counter harvesting attacks*," says Scott Cadzow, the Rapporteur of the Technical Report in the ETSI QSC group.

The migration framework, and the migration plan that documents it, comprises the following three stages:

- **Inventory compilation**
- **Preparation of the migration plan**
- **Migration execution**

The first stage makes the simple point that migration cannot be planned without knowledge of the assets in the organization that will be impacted by a quantum computer. This stage outlines that compiling the inventory is a business process that will require a dedicated manager and a budget assigned to its development and maintenance, recognizing that this may be an extension of existing inventory management with a particular focus on cryptographic properties.

Stage 2 involves detailed planning, and is again treated as a business process. The broad assumption is that migration will be on a like-for-like basis, that an asymmetric cryptographically protected asset will be protected in the same manner after migration, and that symmetric cryptographically protected assets will likewise also be protected in the same manner after migration. However, it has been documented that during migration planning some assets may be substantially redesigned and perhaps even retired.

One aspect stressed in stage 2 is that both migration and initial deployment designs will achieve the same end point but migration differs only insofar as there is an existing working deployment to support business functions sensitive to disruption. The role of stage 2 is to ensure that the entire business is aware of the migration and that its importance is recognized.

The final stage 3 is the turnkey element of the migration itself. The ETSI Report offers a series of checklists to address the management and planning of migration in some detail.

36 First quantum algorithm to characterize noise

https://www.swissquantumhub.com/first-quantum-algorithm-to-characterize-noise/

Researchers at University of Sydney Nano Institute have developed the first system-wide quantum algorithm to characterize noise.

Noise is the main obstacle to building large-scale quantum computers. To tame the noise (interference or instability), scientists need to understand how it affects an entire quantum system. Until now, this information was only available for very small devices or subsets of devices.

The team has developed algorithms that work across large quantum devices. They demonstrated this by diagnosing the noise in an IBM Quantum Experience device, discovering correlations in the 14-qubit machine not previously detected.

37 QUANTUM COMPUTING BREAKTHROUGH AS SCIENTISTS FIND POSSIBLE SOLUTION TO TECHNOLOGY'S BIGGEST HURDLE

by Andrew Griffin

https://www.independent.co.uk/life-style/gadgets-and-tech/news/quantum-computing-computer-noise-algorithm-large-system-ibm-a9663461.html

Scientists have made a major breakthrough in the development of large-scale quantum computers.

"Noise" remains the biggest problem for the development of quantum computers, and must be solved before they can be used widely and in the revolutionary ways that have been proposed. The new paper suggests a way of dealing with such noise, in turn potentially opening up a way to control that noise and develop much better quantum computing systems.

Quantum computers could potentially change the way we use technology, by allowing for the solving of problems that are impossible using today's computers. But, to do so, they need weak enough noise as to be reliable.

The problem of noise remains central to creating working and useful quantum computers. In short, it is a result of the errors that are introduced as quantum scientists manipulate the "qubits" that power a quantum computer, and so that noise must be eliminated before any system can be reliably used.

The noise becomes more of a problem the more qubits there are, and the larger the system, meaning that the problem is a particular barrier for building the kinds of big quantum computers that have been offered as offering revolutionary new technology in the future.

To be able to do that, scientists need to be able to understand how noise functions across a quantum system. Until now, they have only bee able to do so using very small devices.

But new research, published in Nature Physics, includes new algorithms that are able to work in much larger-scale quantum computing devices.

And it has already been successfully used on the IBM Quantum Experience, an online platform that allows researchers to make use of the companies' quantum computing systems.

They found that the algorithm was able to successfully diagnose the noise in the system – finding issues that had not previously been detected.

If quantum computers are to be successful, they will need to be precisely calibrated to avoid noise, or errors. But they will also need to be able to correct those errors if they are to be relied on for important calculations.

To be able to do that, quantum scientists will need to be able to know where the errors are likely to be introduced. Knowing that will allow them to optimise their error correction for the specific problems, rather than doing so in a generic way.

The new breakthrough algorithm allows scientists to better know how many of those errors there should be, and where they might arise, which could be included within future devices to allow them to better correct errors.

"This protocol opens myriad opportunities for novel diagnostic tools and practical applications," the researchers write in the new paper, pointing out that it could be used in a variety of ways to make quantum computers better at handling the noise they generate.

"The results are the first implementation of provably rigorous and scalable diagnostic algorithms capable of being run on current quantum devices and beyond," said Robin Harper, from the University of Sydney, who is lead author on the new paper.

'Efficient learning of quantum noise' is published today in Nature Physics.

10 Aug 2020

38 NSF Rolls Out Beta Quantum Site to Help U.S. Get Quantum Ready

https://thequantumdaily.com/2020/08/10/nsf-rolls-out-beta-quantum-site-to-help-u-s-get-quantum-ready/

The National Science Foundation said their beta website is a small step to prepare us for living "in a quantum future."

The organization announced the site, which introduces people to big ideas in quantum science and quantum information science.

The organization says that the site is needed because the quantum era is dawning – and, although, it will take time, it's necessary to understand the technology now.

"Sooner than we may once have imagined, new technologies will leverage quantum properties to create faster, more secure communications, powerful computers, sophisticated and compact sensors, and even new industrial materials. These developments, rooted in quantum discoveries, hold the potential to stimulate economic growth, strengthen national security, and improve the health and well-being of individuals around the world. But just how distant is this future, and what will it take to get there?"

The site includes a history of quantum and a brief overview of quantum technology.

Critical for the NSF – and for the United States, in general – is to have workers and scientists trained in quantum science.

The organization writes: "Making the quantum future a reality is a goal that researchers around the globe have long been working toward. Quantum is still an emerging area of science, and building technologies that harness its potential will require extensive, fundamental research to better understand the principles that drive it. The U.S. also needs a significantly larger, quantum-educated science and engineering workforce ready to develop, operate and maintain the quantum technologies of the future."

This is just one project that's part of a much larger NSF outreach efforts aimed at quantum. For example, the NSF is investing millions on research institute and quantum ediucation.

"In just the past month, NSF devoted $75 million to create new inter-disciplinary research institutes that address some of the most pressing topics in quantum information science and also invested$9.75M in awards to recruit quantum computing and information science faculty. Recently, NSF, with the White House Office of Science and Technology Policy, announced the National Q-12 Education Partnership, a ground-breaking plan to help young students become quantum learners."

39 QUANTUM DEVICES SUCCESSFULLY BUILT FOR QUBIT C-ONTROL

Press release from Archer

https://www.quantaneo.com/%E2%80%8BQuantum-devices-successfully-built-for-qubit-control_a567.html

Archer Materials Limited is pleased to announce the Company has successfully built the quantum devices required for initial qubit control measurements as part of a significant phase in its technology development related to the operation of the 12CQ room-temperature quantum computing qubit processor.

- Qubit control devices have been built for quantum control measurements to characterise Archer's unique 12CQ qubit processor chip components.
- Archer and the Company's collaborators rapidly developed qubit control devices 'end-to-end' using in-house expertise and local world-class facilities.
- Quantum control measurements are a world-first and successful development would be early-stage validation of 12CQ chip operation.
- 12CQ chip build is advancing, recently achieving key disruptive early-stage technology milestones in the global quantum computing economy.

Commenting on the Company's 12CQ chip development, Archer CEO Dr Mohammad Choucair said: "We commenced our technology development related to qubit control a few weeks ago and now the first devices have been built to perform the initial [qubit control] measurements related to Archer's 12CQ chip operation. We have remained on track in our development since we first commenced the project in April 2019."

"Qubit control is explicitly our next big technological milestone. Over the coming months, Company shareholders will expect to see a series of results that will be released to ASX by Archer that relate to

qubit control – a key requirement of quantum computing processors. When successful, the work would be major validation, at a relatively early-stage of the overall development of a quantum computing processor, of the commercial viability of the 12CQ chip".

The Archer team has built and begun testing prototype qubit control devices in Sydney with collaborating institutes. The initial prototyped ESR device has the primary benefit of providing the magnetic ultra-sensitivity to establish quantitative measurements (i.e. characterisation) of the quantum information residing on very few qubit material components.

The initial ESR device design is intended to allow for qubit control measurements only at low temperatures to maximise the Primary Benefit, with the associated operation temperatures unrelated to Archer's qubits' demonstrated potential to operate at room temperature. The ESR device assembly is unique and unoptimised, subject to changing functional configurations.

40 How a Decentralized Randomness Beacon Could Boost Cryptographic Security

by Alyssa Hertig

https://www.coindesk.com/how-a-decentralized-randomness-beacon-could-boost-cryptographic-security

Key takeaways:

- The League of Entropy is launching the first production-ready version of drand, a network that produces "randomness" (also known as entropy) for anyone to use.
- Randomness is essential to cryptographic security.
- Filecoin is the first protocol to use this version of drand in its upcoming mainnet launch to create decentralized, verifiable randomness for "leader selection."

A novel cryptography piece, which could be of help to many cryptocurrency projects, is officially launching in production today.

The League of Entropy, which was launched last year, is opening the first production-ready version of drand, a network that produces "randomness" (also known as entropy) for anyone to use. Cryptography uses math and puzzles to secure communication in a way that snoops can't untangle. Randomness is an essential piece of cryptography that ensures security by adding unpredictable information to the mix.

What is entropy (or randomness)?

Randomness is data produced in an unpredictable way. One example is rolling a six-sided dice. Before rolling it, you can't predict which of the six numbers will appear.

You can even join together many dice rolls into a string of numbers. The more dice rolls done in a row, the more random and unpredictable the value.

A beacon is a randomness generator that shoots out random numbers at regular intervals, which anyone can look at and verify.

League of Entropy's drand beacon network is unique in that it generates randomness in a new way that doesn't rely on a single point of failure.

It's analogous to having several dice rollers generating numbers and stringing them together, so no single one needs to be trusted.

The founding members, who will be running the beacon, are Cloudflare, École polytechnique fédérale de Lausanne (EPFL), Kudelski Security, Protocol Labs, and the University of Chile. Current membership has expanded to include C4DT, ChainSafe, cLabs, Emerald Onion, the Ethereum Foundation, IC3, PTisp, Tierion and UCL.

At first an experimental project, League of Entropy is now launching drand in production for use on living and breathing projects. Filecoin, a decentralized storage network, will be the first to use the randomness generated by League of Entropy as an integral piece of its network.

"There is simply no public service at the moment that provides the necessary guarantees that multiple applications that use randomness need," Protocol Labs research scientist Nicolas Gailly told CoinDesk. Protocol Labs is the research and development organization behind Filecoin, which aims to "radically improve the internet."

The researchers behind the network have big plans for it: They see it becoming as important as other protocols underpinning the internet today. (Of course, whether it becomes that big remains to be seen.)

Why randomness?

Randomness is a crucial part of cryptography.

When you generate a private key for bitcoin or another a cryptocurrency, randomness is an essential ingredient. It is a component that wallets generally generate behind the scenes with the help of math.

Randomness helps to ensure that no one else can guess what your private key is.

"Intuitively, this is why randomness is crucial in cryptographic applications – because it provides a way to create information that an adversary can't learn or predict," as a research paper on randomness from IEEE Security & Privacy magazine puts it.

For another example, Cloudflare famously uses a wall of lava lamps to produce the randomness it uses to secure a large swathe of the internet.

Public vs. private randomness

The type of randomness used in private keys is supposed to stay private, of course. Exposing the randomness could make it possible to figure out the full private key, leading the user to lose their cryptocurrency.

There's another, different type of randomness that League of Entropy uses – public randomness. This is useful for many other applications where the random numbers produced need to be verified by the public and can be verified by whoever looks at the website.

An example of where this can come in handy is a typical lottery, where the winners are chosen by supposedly random draws from a hat.

The problem is that lotteries have been gamed by the creators over the years, especially in cases where the creator has some control over the randomness generation process. It helps to have a beacon that chooses these random numbers, rather than a less public entity, as it makes it harder to game.

There are various ways to generate public randomness today. One such trusted source of randomness is the National Institute of Standards Technology (NIST).

But there is still one problem: Generally, you still have to trust the entity, whether NIST or some other organization, that generates the randomness.

That is where drand comes in. It's a beacon generating randomness but in a decentralized way, to the extent that the several members composing League of Entropy are providing the randomness. If all goes according to plan, you won't have to trust one single entity, such as NIST. The idea is that it's less likely the organizations comprising the league will collude.

"Today, randomness beacons generate numbers for lotteries and election audits – both affect the lives and fortunes of millions of people. Unfortunately, exploitation of the single point of origin of these beacons have created dishonest results that benefited one corrupt insider. To thwart exploitation efforts, Cloudflare and other randomness-beacon providers have joined forces to bring users a quorum of decentralized randomness beacons. After all, eight independent globally distributed beacons can be much more trustworthy than one!" reads the blog post announcing League of Entropy in 2019.

"There is no other production-ready randomness beacon that combines the guarantees of drand: publicly verifiable, decentralized and unbiasable," Gailly added.

Drand meets Filecoin

This "beacon" can be used for all sorts of applications, from election auditing, to lotteries, to cryptocurrency.

Filecoin is the first project to give the LoE beacon a whirl in Filecoin's attempt at making the internet better. Filecoin is in the midst of preparation for a mainnet launch, after several delays.

Bitcoin miners are more likely to win block rewards if they have more mining hardware and computational power. By contrast, miners in Filecoin are more likely to win block rewards if they have more storage space to contribute to the network.

The process of selecting a miner who wins each block reward is known as "leader selection." Filecoin will be using randomness generated by the League of Entropy for this so-called "leader generation."

"Being able to verify the validity of the randomness, that it's actually correctly generated, is a crucial property for leader election in blockchains," Gailly said.

They launched the League of Network beacon to accomodate all of these use cases.

"Drand's largest deployment, the League of Entropy Mainnet, is a network specialized in generating randomness that can serve many applications rather than being tailored or embedded in just one application," said David Dias, research engineer at Protocol Labs and the drand project lead.

"The League of Entropy is creating the basis for future systems to leverage trustworthy public randomness online, and the new collaborative governance will only improve its ability to do so. We're excited to watch drand help prevent bias and detect manipulation in elections, lotteries, and distributed ledger platforms, and improve the Internet for generations to come," said Cloudfare head of research Nick Sullivan in a statement.

09 Aug 2020

41 Quantum Computers Will No Longer Threat To Bitcoin!

by Leonard Manson

https://www.somagnews.com/quantum-computers-will-no-longer-threat-to-bitcoin/

A new computing software could free Bitcoin and cryptocurrencies from powerful quantum computers that have the potential to violate public key cryptography.

According to the MIT Technology Review, the researchers are working on the development of a new measure known as lattice-based cryptography that promises to make crypto technology more "quantum proof".

Bitcoin and Cryptocurrencies will be Protected

Lattice-based cryptography can neutralize the enormous computational capabilities of quantum computers by hiding data inside complex geometric structures containing a grid of infinite dots spread over thousands of dimensions. The security measure seems almost impenetrable, even with the use of powerful quantum computers, unless the key is in hand.

The advent of quantum computing machines is often brought to the fore as it poses a threat to cryptocurrencies such as Bitcoin as well as cryptographic algorithms that keep the internet generally safe. The World Economic Forum explains how quantum computers can violate current encryption standards as follows.

"The full computational ability of a sufficiently powerful and error-corrected quantum computer means that public-key cryptography is" doomed "and will compromise the technology used to protect many of today's fundamental digital systems and activities.

MIT Technology Review says the solution is promising, although the current iterations are not yet ready to be implemented. Ripple CTO David Schwartz says that developers believe it will take at least eight years before the technology that uses the properties of quantum physics to make quick calculations becomes sophisticated enough to crack the cryptocurrency.

"I think we have at least eight years. I have very high confidence that quantum computing needs at least ten years to pose a threat, but you never know when there might be progress."

08 Aug 2020

42 Silq – A New High Level Programming Language for Quantum Computing

by Michael Lyam

https://thequantumdaily.com/2020/08/08/silq-a-new-high-level-programming-language-for-quantum-computing/

When it comes to programming languages, the first name that comes to mind typically is C. Dating back to the '70s when it was developed at AT&T Bell Laboratories by Dennis Ritchie and Ken Thompson, it was easy to learn by those who wanted to work on computer coding. Most existing computer programs

were written in assembly language, communicating directly with hardware but being complex, long, and hard to debug. C offered ease and intuitiveness of use and brought in a totally new audience to computer programming.

Working with the full potential of quantum computing requires two things:

- The most current technology
- A quantum programming language to describe quantum algorithms

Essentially, while the algorithm explains how to solve a problem, the programming language helps the computer to perform the necessary calculations by describing the algorithm.

Present approaches to quantum computation look to adapt and use existing tools and technologies, as this would allow them to be run on devices that will be available over the next few years. Current quantum languages are somewhat similar to assembly languages in their expressiveness, as the programmer must provide every operation the computer is to perform. The former is also at a lower level than the latter in some respects – chiefly, in describing operations on individual quantum bits, more like what low-level hardware description languages do. Another shortcoming is how closely they are tied to specific hardware, describing the behavior of underlying circuits precisely and thereby requiring highly-detailed individual programming instructions describing the required minutiae. Given the complexity of current programming languages for quantum computers, a new language is needed.

This is how **Silq** came about. It was created by researchers at ETH Zurich, Switzerland, and is claimed to be the first high-level quantum language in the world. Classical and quantum languages are currently quite far apart in their conceptual bases, and Silq looks to bridge that gap, offering an approach that is far more intuitive than imagined. And given how quantum computing could revolutionize AI, Silq could be a very useful programming language for AI.

Silq offers several advantages, some of which are detailed below:

- A level of abstraction close to that of C
- Better usage of the potential of quantum computers than existing languages
- The code used by Silq is more compact, faster, more intuitive, and easier to understand for programmers.
- Existing quantum languages make it difficult to directly support subexpressions such as (a+b) + c, which are directly supported by Silq.
- It facilitates the expression of the high-level intent of programmers through a descriptive view of quantum algorithms. A specialized compiler can take care of compiling these algorithms to low-level quantum circuits.
- Programs in Silq are less-focused on low-level details, which makes analyzing such programs easier than the programs written in existing quantum languages.
- Silq could facilitate the development of tools for analysis to support developers.

What keeps Silq ahead of other languages is its design. It is the first programming language for quantum computing whose design does not limit its focus to the construction and functionality of underlying hardware. The design instead pays due consideration to the mindset of a programmer when a problem is to be solved, and helps in finding a solution that does not need the understanding of each detail of the architecture and implementation of the computer.

Silq falls into the category of high-level programming languages, as it abstracts from technical details of a particular type of computer. It is the first such language for quantum computers, and is more expressive as it can use much lesser code to describe more complex algorithms and tasks. This is why programmers find it easier to comprehend and use, also because it works with different computer architectures.

Possibly the most important innovation of Silq is in dealing with a particular common source of errors. More than one intermediary step makes up the process of calculating a task by a computer, in which process intermediate results or temporary values are created. Classical computers automatically get rid of these values in what is known as a process of "garbage collection", which however is dicey for quantum computers, as previously-calculated values can interfere with correct calculations due to interactions with current values (which is also called quantum entanglement). This requires an uncomputation technique that is more advanced, and Silq allows such identification and erasure automatically.

Silq is definitely a way ahead and is attracting more attention from computer scientists working on usable ideas. Given how it is easier to use, it could stimulate the development of further languages and algorithms for quantum computers.

43 China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI

by Catalin Cimpanu

https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/

The Chinese government is currently using the Great Firewall censorship tool to block certain types of encrypted HTTPS connections.

The block has been in place for more than a week, according to a joint report authored by three organizations tracking Chinese censorship – iYouPort, the University of Maryland, and the Great Firewall Report.

ZDNet also confirmed the report's findings with two additional sources – namely members of a US telecommunications provider and an internet exchange point (IXP) – using instructions provided in a mailing list.

Neither of the two sources wanted their identities and employers named due to China's known habit of direct or indirect reprisals against entities highlighting its internet censorship practices.

CHINA NOW BLOCKING HTTPS+TLS1.3+ESNI

Per the report, China's Great Firewall (GFW) is now blocking HTTPS connections set up via the new TLS 1.3 encryption protocol and which use ESNI (Encrypted Server Name Indication).

The reason for the ban is obvious for experts.

HTTPS connections negotiated via TLS 1.3 and ESNI prevent third-party observers from detecting what website a user is attempting to access. This effectively blinds the Chinese government's Great Firewall surveillance tool from seeing what users are doing online.

There is a myth surrounding HTTPS connections that network observers (such as internet service providers) cannot see what users are doing. This is technically incorrect.

While HTTPS connections are encrypted and prevent network observers from viewing/reading the contents of an HTTPS connection, there is a short period before HTTPS connections are established when third-parties can detect to what server the user is connecting.

This is done by looking at the HTTPS connection's SNI (Server Name Indication) field.

In HTTPS connections negotiated via older versions of the TLS protocol (such as TLS 1.1 and TLS 1.2), the SNI field is visible in plaintext.

In TLS 1.3, a protocol version launched in 2018, the SNI field can be hidden and encrypted via ESNI.

As the TLS 1.3 protocol is seeing broader adoption today, ESNI usage is increasing as well, and more HTTPS connections are now harder to track for online censorship tools like the GFW.

According to iYouPort, the University of Maryland, and the Great Firewall Report, the Chinese government is currently dropping all HTTPS connections where TLS 1.3 and ESNI are used and temporarily blocking the IP addresses involved in the connection for between two and three minutes – depending on the location of the Great Firewall where the "unwanted" connection settings are detected.

SOME CIRCUMVENTION METHODS EXIST ... FOR NOW

Luckily for app makers and website operators catering to Chinese audiences, the three organizations said they found six circumvention methods that can be applied client-side (inside apps and software) and four that can be applied server-side (on servers and app backends) to bypass the Great Firewall's current block.

"Unfortunately, these specific strategies may not be a long-term solution: as the cat and mouse game progresses, the Great Firewall will likely to continue to improve its censorship capabilities," the three organizations wrote in their joint report.

07 Aug 2020

44 World's First Development and Demonstration of a Quantum Cryptographic Communication Technology Applied System for Genomic Medicine)

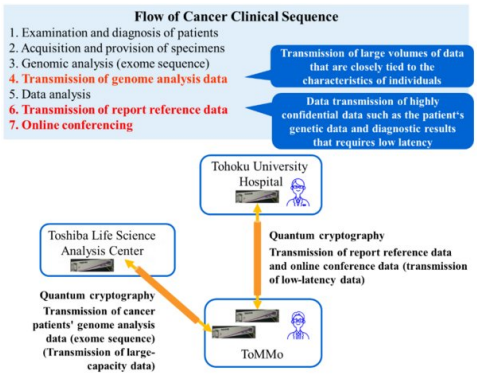
by Toshiba

https://en.prnasia.com/releases/apac/world-s-first-development-and-demonstration-of-a-quantum-cryptographic-communication-technology-applied-system-for-genomic-medicine-28shtml

Toshiba Corporation, Tohoku University Tohoku Medical Megabank Organization (ToMMo) and Tohoku University Hospital have demonstrated that quantum cryptographic communications technology can provide genomic medicine with a safe, completely secure data management environment. This was achieved by

(1) developing a system which applies quantum cryptographic communications technology to clinical sequencing, and

(2) using that system to safely transmit cancer genome analysis data (exome sequence[1] data), via online expert panel attended by physicians and other experts to analyze the sequenced data.



This is the world's first development and demonstration of a system using quantum cryptographic communication technology in the field of genomic medicine[2].

Clinical sequencing is a new examination in genomic medicine that uses a next-generation sequencer to read a patient's gene sequence at ultra-high speed. The results of the genomic data analysis are then provided to physicians and other experts to assist in patient diagnosis and treatment selection. This system builds on and extends capabilities that Toshiba and ToMMo announced in January of this year, and the achievements of this demonstration are a major step toward a practical system that will provide safe and secure genomic medicine.

This research was carried out as part of the Strategic Innovation Creation Program (SIP) of the Council for Science and Technology and Innovation of the Cabinet Office, "Society 5. 0 Realization Technology Utilizing Light and Quantum" (Quantum Science and Technology Research and Development Organization). Toshiba, ToMMo and Tohoku University Hospital will present the details of the demonstration and the technology at the International Conference QCrypt 2020 (10th International Conference on Quantum Cryptography) on August 10-14.

Details

In January this year, Toshiba and ToMMo announced on a series of experiments of quantum cryptography transmission that took place in July and August 2019 that succeeded in transmitting whole-genome sequence data for the first time anywhere in the world[3]. Since then, and joined by Tohoku University Hospital, they have advanced the research by focusing on two areas related to clinical sequencing of cancer patients: the type of data that must be kept confidential; and methods to utilize quantum cryptographic technology in data decryption.

[1] A technique that efficiently detect mutations (SNV (SNP)/InDel) in exons by limiting sequencing to exons, the portion of the gene that code for proteins. This differs from whole-genome sequencing which analyzes the entire genome sequence, and to SNP arrays which comprehensively analyze the existing SNPs on the whole-genome.

[2] Based on Toshiba's internal investigation in July 2020

[3] "World-first Demonstration of Real-time Transmission of Whole-genome Sequence Data Using Quantum Cryptography", announced on January 14, 2020.

Clinical sequencing covers genome analysis data which is highly confidential personal information closely related to one's health and physical condition that must be kept secure. For the same reason, support is also needed for the data generated by online expert panel attended by physicians and experts who share patient's genetic data and diagnostic results via remote access.

After considering this, Toshiba, ToMMo and Tohoku University Hospital successfully demonstrated encryption in two areas using quantum cryptographic communication technology:

(A) Real-time transmission of genome analysis data (exome sequencing data)

(B) Data transmission for an online expert panel, including analyzing results over conference audio and visual feeds.

06 Aug 2020

45 Massive 20GB Intel IP Data Breach Floods the Internet, Mentions Backdoors (Intel Responds)

by Paul Alcorn

https://www.tomshardware.com/news/massive-20gb-intel-data-breach-floods-the-internet-mentions-backdoors

Till Kottmann, a Swiss IT consultant, posted on Twitter a link to a file sharing service today that contains what an anonymous source claims is a portion of Intel's crown jewels: A 20GB folder of confidential Intel intellectual property. The leaker dubbed the release the " Intel exconfidential Lake Platform Release)."

"We are investigating this situation. The information appears to come from the Intel Resource and Design Center, which hosts information for use by our customers, partners and other external parties who have registered for access. We believe an individual with access downloaded and shared this data."

Intel's Resource and Design Center is a website dedicated to providing the company's partners with NDA documentation for product integration purposes. Reports are also cropping up that some of the files are marked with NDA license agreements to " Centerm Information Co. Ltd., a Chinese company established and existing under the laws of the People's Republic of China," meaning this company could have been also hacked.

The folder appears to have been originally posted by an anonymous source that claims more is coming soon, and while we don't know the exact specifics of the folder's contents, we have verified that it does exist. In fact, the title of many of the documents do correlate to the list of purported information posted by the leaker:

- Intel ME Bringup guides + (flash) tooling + samples for various platforms
- Kabylake (Purley Platform) BIOS Reference Code and Sample Code + Initialization code (some of it as exported git repos with full history)
- Intel CEFDK (Consumer Electronics Firmware Development Kit (Bootloader stuff)) SOURCES
- Silicon / FSP source code packages for various platforms

- Various Intel Development and Debugging Tools
- Simics Simulation for Rocket Lake S and potentially other platforms
- Various roadmaps and other documents
- Binaries for Camera drivers Intel made for SpaceX
- Schematics, Docs, Tools + Firmware for the unreleased Tiger Lake platform (very horrible) Kabylake FDK training videos
- Intel Trace Hub + decoder files for various Intel ME versions
- Elkhart Lake Silicon Reference and Platform Sample Code
- Some Verilog stuff for various Xeon Platforms, unsure what it is exactly.
- Debug BIOS/TXE builds for various Platforms
- Bootguard SDK (encrypted zip)
- Intel Snowridge / Snowfish Process Simulator ADK
- Various schematics
- Intel Marketing Material Templates (InDesign)
- Lots of other things

Kottman, who has been behind other data dumps of proprietary information in the past, claims the hacker " breached" Intel, which the company denies. Kottman also said the files were obtained earlier this year, adding " most of the things here have NOT been published ANYWHERE before and are classified as confidential, under NDA or Intel Restricted Secret." The source says more files will be shared soon, and " the future parts of this leak will have even juicier and more classified stuff."

Interestingly, Kottman also notes " If you find password protected zips in the release the password is probably either " Intel123" or " intel123". This was not set by me or my source, this is how it was acquired from Intel."

The posts encourage downloaders to look for mentions of 'backdoors' in some of the Intel source code, and even provides a sample clip of one such listing, but we aren't sure of the intentions behind the listings in the code.

The link is being widely distributed on Twitter, but it might be best to exercise caution – downloading any file from an untrusted source is always a risk.

46 Insecure satellite Internet is threatening ship and plane safety

by DAN GOODIN

https://arstechnica.com/information-technology/2020/08/insecure-satellite-internet-is-threatening-ship-and-plane-safety/

More than a decade has passed since researchers demonstrated serious privacy and security holes in satellite-based Internet services. The weaknesses allowed attackers to snoop on and sometimes tamper with data received by millions of users thousands of miles away. You might expect that in 2020 – as satellite Internet has grown more popular – providers would have fixed those shortcomings, but you'd be wrong.

In a briefing delivered on Wednesday at the Black Hat security conference online, researcher and Oxford PhD candidate James Pavur presented findings that show that satellite-based Internet is putting millions of people at risk, despite providers adopting new technologies that are supposed to be more advanced.

Over the course of several years, he has used his vantage point in mainland Europe to intercept the signals of 18 satellites beaming Internet data to people, ships, and planes in a 100 million-square-kilometer swath that stretches from the United States, Caribbean, China, and India. What he found is concerning. A small sampling of the things he observed include:

- A Chinese airliner receiving unencrypted navigational information and potentially avionics data. Equally worrisome, that data came from the same connection passengers used to send email and browse webpages, raising the possibility of hacks from passengers.
- A system administrator logging in to a wind turbine in southern France, some 600 kilometers away from Pavur, and in the process exposing a session cookie used for authentication.
- The interception of communications from an Egyptian oil tanker reporting a malfunctioning alternator as the vessel entered a port in Tunisia. Not only did the transmission allow Pavur to know the ship would be out of commission for a month or more, he also obtained the name and passport number of the engineer set to fix the problem.
- A cruise ship broadcasting sensitive information about its Windows-based local area network, including the log-in information stored in the Lightweight Directory Access Protocol database
- Email a lawyer in Spain sent a client about an upcoming case.
- The account reset password for accessing the network of a Greek billionaire's yacht.

Hacking satellite communications at scale

While researchers such as Adam Laurie and Leonardo Nve demonstrated the insecurity of satellite Internet in 2009 and 2010, respectively, Pavur has examined the communications at scale, with the interception of more than 4 terabytes of data from the 18 satellites he tapped. He has also analyzed newer protocols, such as Generic Stream Encapsulation and complex modulations including 32-Ary Amplitude and Phase Shift Keying (APSK). At the same time, he has brought down the interception cost of those new protocols from as much as $50,000 to about $300.

"There are still many satellite Internet services operating today which are vulnerable to their [the previous researchers'] exact attacks and methods – despite these attacks having been public knowledge for more than 15 years at this point," Pavur told me ahead of Wednesday's talk. "We also found that some newer types of satellite broadband had issues with eavesdropping vulnerabilities as well."

The equipment Pavur used consisted of a TBS 6983/6903 PCIe card/DVB-S tuner, which allows people to watch satellite TV feeds from a computer. The second piece was a flat-panel dish, although he said any dish that receives satellite TV will work. The cost for both: about $300.

Using public information showing the location of geostationary satellites used for Internet transmission, Pavur pointed the dish at them and then scanned the ku band of the radio spectrum until he found a signal hiding in the massive amount of noise. From there, he directed the PCIe card to interpret the signal and record it as a normal TV signal. He would then look through raw binary files for strings such as “http” and those corresponding to standard programming interfaces to identify Internet traffic.

All unencrypted comms are mine

The setup allows Pavur to intercept just about every transmission an ISP sends to a user via satellite, but monitoring signals the other way (from the user to the ISP) is much more limited. As a result, Pavur could reliably see the contents of HTTP sites a user was browsing or of an unencrypted email the user downloaded, but he couldn’t obtain customers’ “GET” requests or the passwords they sent to the mail server.

Even though the customer may be located in the Atlantic off the coast of Africa and is communicating with an ISP in Ireland, the signal it sends is easily intercepted from anywhere within tens of millions of square kilometers, since the high cost of satellites requires providers to beam signals over a wide area.

Pavur explained:

> There are a few reasons the other direction is harder to capture. The first is that the beam connecting a satellite to an ISP’s ground station is often more narrow and focused (meaning you have to be within a few dozen miles of the ISP’s system to pick up radio waves in that direction). In some cases, ISP’s will use a different frequency band to transmit these signals for bandwidth and performance reasons – this means an attack might need equipment that is much harder to pick up commercially and affordably. Finally, even if an ISP just uses a normal wide-beam K¿u-band signal, they will normally transmit on a different frequency in each direction. This means an attacker would need a second set of antennas (not too difficult) and would also need to combine the two feeds correctly (slightly more difficulty).

Et tu, Avionics?

In past years, Pavur focused on transmissions sent to everyday users on land and large ships at sea. This year, he turned his attention to planes. With the onset of the COVID-19 pandemic causing passenger flying to plummet, the researcher had less opportunity than he planned to analyze passenger communications from entertainment systems, in-flight Internet services, and onboard femtocells used to send and receive mobile signals. (He did, however, see a text message providing a passenger with a coronavirus test.)

But it turned out that the decrease in passenger traffic made it easier to focus on traffic sent to crew members in the cockpit. When one of the crew fat fingered a login to what’s known as an electronic flight bag, the flightdeck equipment repeatedly got an HTTP 302 Redirect error to the Wi-Fi service login page. The redirect format included the URL of the original request showing the GET parameters of the flight bag API. The parameters described the specific flight number and its coordinates, information that gave Pavur a good feel for what the device was doing aboard the plane.

The flight-bag data passed through the same network-address-translation router as entertainment and Internet traffic from passengers. In other words, the same physical satellite antenna and modem were delivering Internet traffic to both the flight bag and passengers. This suggests that any network segregation

that may exist was performed by software rather than through physical hardware separation, which is less prone to hacking.

Session hijacking: The attacker always wins

The use of satellite-based Internet to receive the navigational data puts the crew and passengers at risk of an attack Pavur developed that allows an attacker to impersonate the aircraft with which the ground station is communicating. The hack uses TCP session hijacking, a technique in which the attacker sends the ISP the metadata customers use to authenticate themselves.

Because users' traffic is bounced off a satellite 30,000 kilometers above Earth – a route that typically results in signal latency of about 700 milliseconds – and the attacker's data isn't, the attacker will always beat customers in reaching the ISP.

The session hijacking can be used to cause planes or ships to report incorrect locations or fuel levels, false readings for heating, ventilation, and air conditioning systems, or transmit other sensitive data that's falsified. It can also be used to create denials of service that prevent the vessel from receiving data that's crucial to safe operations.

A problem in search of a solution

The common reaction Pavur gets after he shares his findings is that satellite-based Internet users should simply use a VPN to prevent attackers from reading or tampering with any data sent. Unfortunately, he said, the handshakes required for each endpoint to authenticate itself to the other results in a slow-down of about 90%. The overhead increases the already-large 700 millisecond latency to a wait that renders satellite Internet almost completely unusable.

And while HTTPS and transport-level encryption for email prevent attackers from reading the body of pages and messages, most domain-lookup queries continue to be unencrypted. Attackers can learn plenty by scrutinizing the data. HTTPS certificates allow attackers to fingerprint servers customers connect to.

That information allows attackers to identify users who are worthy of more targeted attacks. Out of 100 ships Pavur pseudo-randomly looked at, he was able to deanonymize about 10 and tie them to specific vessels.

The interception of unencrypted navigational charts, equipment failures in the open sea, and the use of vulnerability-riddled Windows 2003 servers also puts users at considerable risk. Combined with the use of insecure channels such as FTP, an attacker might be able to tamper with maritime data to hide a sandbar or use the data to plan physical intrusions.

The sheer scale of the problem put the researcher in a quandary. With tens of thousands of users affected, Pavur was unable to privately notify the vast majority of them. He settled on contacting the largest companies who were transmitting particularly sensitive data in the clear. He ultimately chose not to identify any of the affected users or companies because, he said, the crux of the problem is the result of industrywide protocols that are insecure.

"The goal of my research is to bring out these unique dynamics that the physical properties of space create for cybersecurity, and it's an area that's been underexplored," he said. "A lot of people think that satellites are just normal computers that are a little bit further away, but there's a lot that's different about satellites. If we highlight those differences, we can better build security to protect the systems."

47 A Quintillion Calculations a Second: DOE Calculating the Benefits of Exascale and Quantum Computers

by U.S. DEPARTMENT OF ENERGY

https://scitechdaily.com/a-quintillion-calculations-a-second-doe-calculating-the-benefits-of-exascale-and-quantum-computers/

A quintillion calculations a second. That's one with 18 zeros after it. It's the speed at which an exascale supercomputer will process information. The Department of Energy (DOE) is preparing for the first exascale computer to be deployed in 2021. Two more will follow soon after. Yet quantum computers may be able to complete more complex calculations even faster than these up-and-coming exascale computers. But these technologies complement each other much more than they compete.

It's going to be a while before quantum computers are ready to tackle major scientific research questions. While quantum researchers and scientists in other areas are collaborating to design quantum computers to be as effective as possible once they're ready, that's still a long way off. Scientists are figuring out how to build qubits for quantum computers, the very foundation of the technology. They're establishing the most fundamental quantum algorithms that they need to do simple calculations. The hardware and algorithms need to be far enough along for coders to develop operating systems and software to do scientific research. Currently, we're at the same point in quantum computing that scientists in the 1950s were with computers that ran on vacuum tubes. Most of us regularly carry computers in our pockets now, but it took decades to get to this level of accessibility.

In contrast, exascale computers will be ready next year. When they launch, they'll already be five times faster than our fastest computer – Summit, at Oak Ridge National Laboratory's Leadership Computing Facility, a DOE Office of Science user facility. Right away, they'll be able to tackle major challenges in modelling Earth systems, analyzing genes, tracking barriers to fusion, and more. These powerful machines will allow scientists to include more variables in their equations and improve models' accuracy. As long as we can find new ways to improve conventional computers, we'll do it.

Once quantum computers are ready for prime time, researchers will still need conventional computers. They'll each meet different needs.

DOE is designing its exascale computers to be exceptionally good at running scientific simulations as well as machine learning and artificial intelligence programs. These will help us make the next big advances in research. At our user facilities, which are producing increasingly large amounts of data, these computers will be able to analyze that data in real time.

Quantum computers, on the other hand, will be perfect for modelling the interactions of electrons and nuclei that are the constituents of atoms. As these interactions are the foundation for chemistry and materials science, these computers could be incredibly useful. Applications include modelling fundamental chemical reactions, understanding superconductivity, and designing materials from the atom level up. Quantum computers could potentially reduce the time it takes to run these simulations from billions of years to a few minutes. Another intriguing possibility is connecting quantum computers with a quantum internet network. This quantum internet, coupled with the classical internet, could have a profound impact on science, national security, and industry.

Just as the same scientist may use both a particle accelerator and an electron microscope depending on what they need to do, conventional and quantum computing will each have different roles to play. Scientists supported by the DOE are looking forward to refining the tools that both will provide for research in the

future.

48 Using entangled photons to play “quantum Go”

https://www.swissquantumhub.com/using-entangled-photons-to-play-quantum-go/

A team of researchers affiliated with several institutions in China has developed a form of the board game Go using entanglement.

The researchers created a version of quantum Go using entangled photons and found that in continuously generating entangled photons as play progressed, they were able to introduce a random element to the game, which, they note, is required to build ever more powerful AI systems able to play sophisticated games with an element of randomness, such as poker.

Go has long been considered as a testbed for artificial intelligence. By introducing certain quantum features, such as superposition and collapse of wavefunction, they experimentally demonstrated a quantum version of Go by using correlated photon pairs entangled in polarization degree of freedom. The total dimension of Hilbert space of the generated states grows exponentially as two players take turns to place the stones in time series. As nondeterministic and imperfect information games are more difficult to solve using nowadays technology, they found that the inherent randomness in quantum physics can bring the game nondeterministic trait, which does not exist in the classical counterpart.

Some quantum resources, like coherence or entanglement, can also be encoded to represent the state of quantum stones. Adjusting the quantum resource may vary the average imperfect information (as comparison classical Go is a perfect information game) of a single game. They further verified its nondeterministic feature by showing the unpredictability of the time series data obtained from different classes of quantum state.

Finally, by comparing quantum Go with a few typical games that are widely studied in artificial intelligence, they found that quantum Go can cover a wide range of game difficulties rather than a single point. Their results establish a paradigm of inventing new games with quantum-enabled difficulties by harnessing inherent quantum features and resources, and provide a versatile platform for the test of new algorithms to both classical and quantum machine learning.

05 Aug 2020

49 Beware of find-my-phone, Wi-Fi, and Bluetooth, NSA tells mobile users

by DAN GOODIN

https://arstechnica.com/tech-policy/2020/08/beware-of-find-my-phone-wi-fi-and-bluetooth-nsa-tells-mobile-users/

The National Security Agency is recommending that some government workers and people generally concerned about privacy turn off find-my-phone, Wi-Fi, and Bluetooth whenever those services are not needed, as well as limit location data usage by apps.

"Location data can be extremely valuable and must be protected," an advisory published on Tuesday stated. "It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations."

NSA officials acknowledged that geolocation functions are enabled by design and are essential to mobile communications. The officials also admit that the recommended safeguards are impractical for most users. Mapping, location tracking of lost or stolen phones, automatically connecting to Wi-Fi networks, and fitness trackers and apps are just a few of the things that require fine-grained locations to work at all.

The cost of convenience

But these features come at a cost. Adversaries may be able to tap into location data that app developers, advertising services, and other third parties receive from apps and then store in massive databases. Adversaries may also subscribe to services such as those offered by Securus and LocationSmart, two services that The New York Times and KrebsOnSecurity documented, respectively. Both companies either tracked or sold locations of customers collected by the cell towers of major cellular carriers.

Not only did LocationSmart leak this data to anyone who knew a simple trick for exploiting a common class of website bug, but a Vice reporter was able to obtain the real-time location of a phone by paying $300 to a different service. The New York Times also published this sobering feature outlining services that use mobile location data to track the histories of millions of people over extended periods.

The advisory also warns that tracking often happens even when cellular service is turned off, since both Wi-Fi and Bluetooth can also track locations and beam them to third parties connected to the Internet or with a sensor that's within radio range.

To prevent these types of privacy invasions, the NSA recommends the following:

- Disable location services settings on the device.
- Disable radios when they are not actively in use: disable BT and turn off Wi-Fi if these capabilities are not needed. Use Airplane Mode when the device is not in use. Ensure BT and Wi-Fi are disabled when Airplane Mode is engaged.
- Apps should be given as few permissions as possible:
  - Set privacy settings to ensure apps are not using or sharing location data.
  - Avoid using apps related to location if possible, since these apps inherently expose user location data. If used, location privacy/permission settings for such apps should be set to either not allow location data usage or, at most, allow location data usage only while using the app. Examples of apps that relate to location are maps, compasses, traffic apps, fitness apps, apps for finding local restaurants, and shopping apps.
- Disable advertising permissions to the greatest extent possible:
  - Set privacy settings to limit ad tracking, noting that these restrictions are at the vendor's discretion.
  - Reset the advertising ID for the device on a regular basis. At a minimum, this should be on a weekly basis.
- Turn off settings (typically known as FindMy or Find My Device settings) that allow a lost, stolen, or misplaced device to be tracked.

- Minimize Web browsing on the device as much as possible, and set browser privacy/permission location settings to not allow location data usage.
- Use an anonymizing Virtual Private Network (VPN) to help obscure location.
- Minimize the amount of data with location information that is stored in the cloud, if possible.

If it is critical that location is not revealed for a particular mission, consider the following recommendations:

- Determine a non-sensitive location where devices with wireless capabilities can be secured prior to the start of any activities. Ensure that the mission site cannot be predicted from this location.
- Leave all devices with any wireless capabilities (including personal devices) at this non-sensitive location. Turning off the device may not be sufficient if a device has been compromised.
- For mission transportation, use vehicles without built-in wireless communication capabilities, or turn off the capabilities, if possible.

Mobile phone use means being tracked

Patrick Wardle, a macOS and iOS security expert and a former hacker for the NSA, said the recommendations are a "great start" but that people who follow the recommendations shouldn't consider them anything close to absolute protection.

"As long as your phone is connecting to cell towers, which it has to in order to use the cell network ... AFAIK that's going to reveal your location," Wardle, who is a security researcher at the macOS and iOS enterprise management firm Jamf, told me. "It, as always, is a tradeoff between functionality/usability and security, but basically if you use a phone, assume that you can be tracked."

He said that recent versions of iOS make it easy to follow many of the recommendations. The first time users open an app, they get a prompt asking if they want the app to receive location data. If the user says yes, the access can only happen when the app is open. That prevents apps from collecting data in the background over extended periods of time. iOS also does a good job of randomizing MAC addresses that, when static, provide a unique identifier for each device.

More recent versions of Android also allow the same location permissions and, when running on specific hardware (which usually come at a premium cost), also randomize MAC addresses.

Both OSes require users to manually turn off ad personalization and reset advertising IDs. In iOS, people can do this in Settings ¿ Privacy ¿ Advertising. The slider for Limit Ad Tracking should be turned on. Just below the slider is the Reset Advertising Identifier. Press it and choose Reset Identifier. While in the Privacy section, users should review which apps have access to location data. Make sure as few apps as possible have access.

Change some settings

In Android 10, users can limit ad tracking and reset advertising IDs by going to *Settings ¿ Privacy and clicking Ads*. Both the Reset Advertising ID and Opt Out of Ads personalization are there. To review

which apps have access to location data, go to *Settings ¿ Apps & notifications ¿ Advanced ¿ Permission Manager ¿ Location*. Android allows apps to collect data continuously or only when in use. Allow only apps that truly require location data to have access, and then try to limit that access to only when in use.

Tuesday's advisory also recommends people limit sharing location information in social media and remote metadata showing sensitive locations before posting pictures. The NSA also warns about location data being leaked by car navigation systems, wearable devices such as fitness devices, and Internet-of-things devices.

The advice is aimed primarily at military personnel and contractors whose location data may compromise operations or put them at personal risk. But the information can be useful to others, as long as they consider their threat model and weigh the acceptable risks versus the benefits of various settings.

04 Aug 2020

50 Qrypt's 'Everlasting Security' For Cyberworld

by James Dargan

https://thequantumdaily.com/2020/08/04/qrypts-everlasting-security-for-cyberworld/

With the risk of cybersecurity attacks at an all-time high, quantum computing's potential has come about at just the right time.

Hack Attack

Nothing presents to us the dangers of cybersecurity threats more than the Russian interference in the 2016 United States elections and the Marriott hotel data breach. Though one is political and the other corporate in nature, the damage they have caused is difficult to calculate by mere statistics alone.

As the two examples testify to, people's lives – and their trust – in the technology that somehow 'binds' us has been severely tested numerous times throughout the late 20th and early part of the 21st century.

Now, though the Pentagon and other western democracies would say Russia and its satellites are the cynosures for all this black-hat conjuring of the technological landscape, I seriously doubt that is the case.

China's cloak and dagger tactics and offhanded behaviour are more a threat to the world's security than anything Mr Putin can throw at them.

And the Americans and British have blood on their hands, too.

No One's Innocent

Just last year, the United States ramped up its arsenal of cyber tools on the Russian power grid system in a Trump show of defiance. This 'hack attack' was in response to the Kremlin's constant (according to U.S sources) barrage of cybersecurity attacks.

Another is the Cambridge Analytica scandal. Just look at Alexander Nix, the Eton-educated former CEO of the now-defunct political consulting firm. Born with a platinum spoon in his mouth, he is the

epitome of British upper-class hypocrisy with a 'butter-wouldn't-melt-in-his-mouth' attitude. Think Putin's dangerous? Think again. It's people like Alexander Nix who you have to look out for.

They say there are two sides to every story, and at TQD we tend to believe it because threats can come from anywhere. Think you're okay because you've got eyes in the back of your head? Think again.

But I have, through anger, or malice, or purely fear for the future I see in front of humankind, left the main road and erred somewhat off track.

Sorry about that.

What I'm trying to get at is in the future we will have to rely on better ways to secure the data we own, share and eventually 'do away with'. Yet, I'm sure that won't be possible with the hooded claw at every turn, at least with current cybersecurity solutions.

Computers aren't up to it anymore. Neither even are their more advanced brethren, supercomputers. The magic of bits and bytes is fading, fast. The digital age, at least in regard to cybersecurity issues, is coming to a sad end.

Quantum computers, then, 'could' take cybersecurity solutions to the next level.

Quantum Secure Encryption

At present, the companies in the quantum computing (QC) space whose sole strategy is to advertise, elevate and improve upon current cybersecurity solutions are growing but still modest in number. British startup **ArQit**, **BLAKFX** from the USA, CryptoNext and Crypto Quantuique from France, are just four representatives of the almost thirty quantum security companies currently listed on TQD dataset doing everything to make our future technological experience a safe and enjoyable one.

Another of these, one that is making inroads in cybersecurity issues that will – let us hope – prevent altercations like the Cambridge Analytica debacle ever happening again is busy finding ways to work things out.

And all they want are two things: 'Quantum Secure Encryption' and 'Everlasting Security'.

Qrypt – whose headquarters are located at the One World Trade Center in Lower Manhattan – offers encryption solutions to secure enterprise today and eliminate future risk.

The place in itself is poignant. From the ashes comes the phoenix. Maybe Kevin Chalker and Denis Mandich, co-founders of Qrypt, believe the old replacing the new is symbolically befitting for their startup. Qubits replacing bits. A more secure world, all in all.

Qrypt

Founded in 2017, Qrypt realizes current encryption methods are 'vulnerable and archaic technologies'. Quantum computing, the team believes, will render this technology obsolete and bring in a new world of securer data protection.

> 'QRYPT'S POST QUANTUM SECURE ENCRYPTION PROTECTS DATA INDEFINITELY, DELIVERING EVERLASTING SECURITY AND ULTIMATE PEACE OF MIND.'

CEO and cofounder of Qrypt, Kevin Chalker, has his hand in many pies as far as the startup's direction goes: from coordinating Qrypt's global business development, he also builds strategic partnerships while concentrating his efforts on one of the most important things a startup can do: building client relationships.

⋮

Qrypt is at the right place at the right time, for sure. With a team of experts in hardware, software and product development in a place whose core values are in dedication, flexibility, security, and diversity, the startup from the Big Apple can – through our own insecurities about technology – become a leading force in QC cybersecurity services for a long time to come.

51 Iranian hacker group becomes first known APT to weaponize DNS-over-HTTPS (DoH)

by Catalin Cimpanu

https://www.zdnet.com/article/iranian-hacker-group-becomes-first-known-apt-to-weaponize-dns-over-https-doh/

An Iranian hacking group known as Oilrig has become the first publicly known threat actor to incorporate the DNS-over-HTTPS (DoH) protocol in its attacks.

Speaking in a webinar last week, Vincente Diaz, a malware analyst for antivirus maker Kaspersky, said the change happened in May this year when Oilrig added a new tool to its hacking arsenal.

According to Diaz, Oilrig operators began using a new utility called DNSExfiltrator as part of their intrusions into hacked networks.

DNSExfiltrator is an open-source project available on GitHub that creates covert communication channels by funneling data and hiding it inside non-standard protocols.

As its name hints, the tool can transfer data between two points using classic DNS requests, but it can also use the newer DoH protocol.

Diaz said Oilrig, also known as APT34, has been using DNSExfiltrator to move data laterally across internal networks, and then exfiltrate it to an outside point.

Oilrig is most likely using DoH as an exfiltration channel to avoid having its activities detected or monitored while moving stolen data.

This is because the DoH protocol is currently an ideal exfiltration channel for two primary reasons. First, it's a new protocol that not all security products are capable of monitoring. Second, it's encrypted by default, while DNS is cleartext.

OILRIG HAS A HISTORY WITH DNS EXFILTRATION CHANNELS

The fact that Oilrig was one of the first APTs (Advanced Persistent Threats – a term used to describe government-backed hacking groups) to deploy DoH is also not a surprise.

Historically, the group has dabbled with DNS-based exfiltration techniques. Before adopting the open-source DNSExfiltrator toolkit in May, the group had been using a custom-built tool named DNSpionage since at least 2018, per reports by Talos, NSFOCUS, and Palo Alto Networks.

In the May campaign, Kaspersky said Oilrig exfiltrated data via DoH to COVID-19-related domains.

During the same month, Reuters independently reported about a spear-phishing campaign orchestrated by unidentified Iranian hackers, who targeted the staff pharma giant Gilead, which at the time announced

it began working on a treatment for the COVID-19 virus. It is, however, unclear if these are the same incidents.

Previous reporting has linked most Iranian APTs as working as members or working as contractors for the Islamic Revolutionary Guard Corps, Iran's top military entity.

But while Oilrig is the first publicly reported APT to use DoH, it is now the first malware operation to do so, in general. Godlua, a Lua-based Linux malware strain was the first to deploy DoH as part of its DDoS botnet in July 2019, according to a report from Netlab, a network threat hunting unit of Chinese cyber-security giant Qihoo 360.

52 CWI CRYPTOLOGISTS BRING CRYSTALS-KYBER TO NIST POST-QUANTUM CRYPTOGRAPHY FINAL

by THE QUBIT REPORT

https://qubitreport.com/quantum-computing-cybersecurity-and-cryptography/2020/08/04/cwi-cryptologists-bring-crystals-kyber-to-nist-post-quantum-cryptography-final/

CWI's Léo Ducas involved in finalists of NIST Post-Quantum Cryptography Standardization.

- In order to protect sensitive data against attacks from quantum computers, several approaches of cryptography can be possible. In order to standardize this next-generation cryptography, the National Institute of Standards and Technology (NIST) examines submitted approaches in a competition-like process. Its focus is on public-key encryption schemes and on digital signatures schemes that combine high performance and general purpose with security in the face of possible future quantum computing.

  In its process to develop the first cryptographic standard to protect sensitive electronic data against the threat of quantum computers, the US National Institute of Standards and Technology (NIST) announced the finalists. Léo Ducas from CWI's Cryptology group is involved in several finalists of this standardization process.

- NIST announced a group of seven finalists, on 22 June 2020. CWI researcher Léo Ducas is involved in several of these finalists. He is a co-designer of one of the four finalists for public-key encryption (CRYSTALS-KYBER) and of one of the three finalists for digital signatures (CRYSTALS-DILITHIUM).

- Both proposals are the result of a multi-national collaborative effort, which included CWI, University of Lyon, Radboud University, Ruhr University Bochum, University of Waterloo, IBM, NXP, ARM, and SRI International).

03 Aug 2020

53 Option pricing using Quantum Computers

https://www.swissquantumhub.com/option-pricing-using-quantum-computers/

A team from JPMorgan Chase, IBM Research Zurich and ETH Zurich presents a methodology to price options and portfolios of options on a gate-based quantum computer using amplitude estimation, an algorithm which provides a quadratic speedup compared to classical Monte Carlo methods.

The options that they have covered include vanilla options, multi-asset options and path-dependent options such as barrier options. They put an emphasis on the implementation of the quantum circuits required to build the input states and operators needed by amplitude estimation to price the different option types.

Additionally, they showed simulation results to highlight how the circuits that they implemented price the different option contracts.

Finally, they examined the performance of option pricing circuits on quantum hardware using the IBM Q Tokyo quantum device. They employed a simple, yet effective, error mitigation scheme that allowed them to significantly reduce the errors arising from noisy two-qubit gates.

54 A quantum protocol for sharing a secret amongst many parties

by Amit Malewar

https://www.techexplorist.com/quantum-protocol-sharing-secret-amongst-parties/34239/

Anyone who has sent an email will know that often information must be sent to several people: one sender and many receiving parties. Traditional quantum communication, such as quantum key distribution (QKD), does not allow this and is only of the peer-to-peer form.

Using structured light as quantum photon states, the Wits team showed how to distribute information from one sender to 10 parties. Scientists at the University of the Witwatersrand in Johannesburg, South Africa, have demonstrated a record-setting quantum protocol for sharing a secret amongst many parties.

By using quantum tricks, the secret can only be unlocked if the parties trust one another.

Professor Andrew Forbes from the School of Physics at Wits University said, "In essence, each party has no useful information, but if they trust one another, then the secret can be revealed. The level of trust can be set from just a few of the parties to all of them. Importantly, at no stage is the secret ever revealed through communication between the parties: they don't have to reveal any secrets. In this way, a secret can be shared in a fundamentally secure manner across many nodes of a network: quantum secret sharing."

"Our work pushes the state-of-the-art and brings quantum communication closer to true network implementation. When you think of networks, you think of many connections, many parties, who wish to share information and not just two. Now we know how to do this the quantum way."

Using structured photons, scientists were able to reach high dimensions. Structured light means 'Patterns of light,' and here, the team could use many patterns to push the dimension limit. More dimensions mean more information in the light and translate directly to larger secrets.