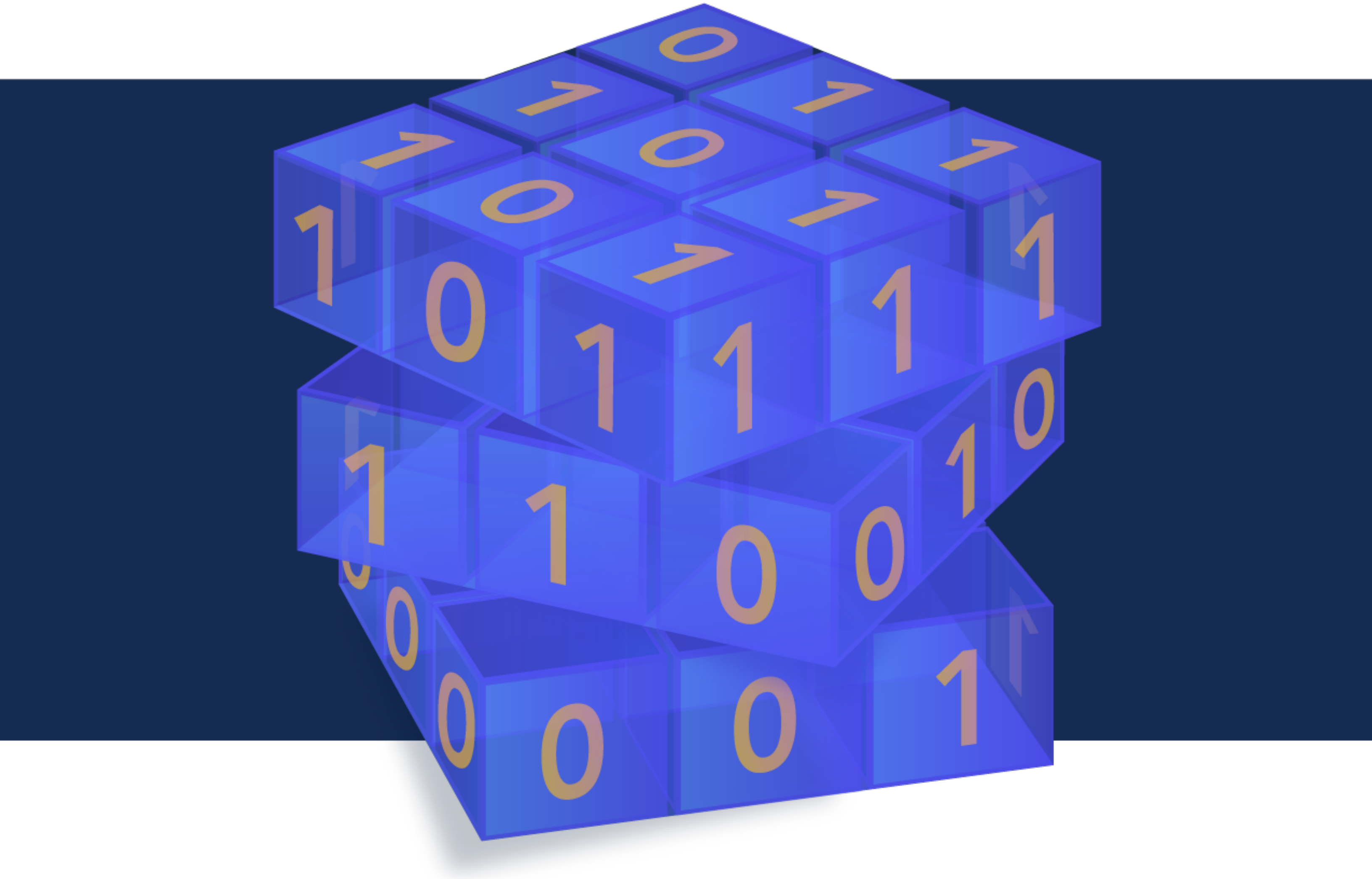
Crypto News

Compiled by Dhananjoy Dey, Indian Institute of Information Technology, Lucknow, U. P. - 226 002, India, ddey@iiitl.ac.in

February 01, 2022



1.IBM Unveils 127-Qubit Quantum Computer 5

2.Department of Space demonstrates entanglement based quantum communication over 300m free space along with real time cryptographic applications 6

3.Quantum Computing Threatens Everything — Could it be Worse Than the Apocalypse? 7

4.Why Gate-Level Quantum Design is Becoming Impossible 10

5.Will quantum computing help or hinder the fight against cybercrime? 11

6.How big does your quantum computer need to be? 14

7.A new language for quantum computing 16

8.Twin-field quantum key distribution (QKD) across an 830-km fibre 18

9.The Biden White House Gets Quantum Right—At Last 20

10.Research demonstrates a new technique for improving long-distance quantum key distribution in a real-world field22

11.The race for quantum-resistant cryptography 23

12.Nuclear quantum computing: It’s coming 27

13.Groundbreaking light sources can increase effectiveness and security of transferring quantum information 29

14.Quantum computing is coming. Now is the right time to start getting ready 30

15.European Milestone: Quantum Computer With More Than 5,000 Qubits Launched 33

16.Towards compact quantum computers, thanks to topology 35

17.DoNot Hacking Team Targeting Government and Military Entities in South Asia 37

18.Inner workings of quantum computers 38

19.How France Is Becoming a Quantum Computing Power 40

20.Israeli quantum cryptographic solutions provider QuantLR integrates with NVIDIA 41

21.Major Breakthrough As Quantum Computing in Silicon Hits 99% Accuracy 42

22.Innovative New Algorithms Advance the Computing Power of Early-Stage Quantum Computers 44

23.Securing IoT with Quantum Cryptography 45

24.Finland moves to industrialise quantum computing 46

25.Log4j: Google and IBM call for list of critical open source projects 50

26.Researchers May Have a Method to Keep Quantum Information as Safe as Classical Information 52

27.Indian Researchers Say Cold Atom Spin Coherence Work Could Help Quantum Computing 53

28.Capgemini launches a dedicated Quantum Lab and announces a new agreement with IBM to advance industry applications of quantum computing 54

29.CISA alerts federal agencies of ancient bugs still being exploited 56

30.9 ways that cybersecurity may change in 2022 57

31.Last year was a record year for attacks, and Log4J made it worse 59

32.Cellframe Network: Post-Quantum Encryption and Decentralized Applications 61

33.IBM Welcomes LG Electronics to the IBM Quantum Network to Advance Industry Applications of Quantum Computing 63

34.Making Next Generation Quantum Computers Even More Powerful 64

35.Tech you need to know: homomorphic encryption 65

36.Cybersecurity training isn't working. And hacking attacks are only getting worse 67

37.Strangeworks, Quantinuum Work Together on Quantum-Enhanced Cryptographic Key Service 68

38.Google's 2021 Year in Review lays out hopes for practical quantum computing this decade 69

39.Cyberattack against UK Ministry of Defence training academy revealed 71

40.New Standards Rolling Out for Clocking Quantum Computer Performance 72

41.QUANTUM RESISTANCE: TAKING PROOF OF KEYS DAY TO THE NEXT LEVEL 74

42.Ten cybersecurity resolutions for a safer 2022 76

43.Quantum technology: how it works, applications and why the US and China are racing to achieve supremacy 78

44.QUANTUM COMPUTING in 2022: A LEAP into THE TREMENDOUS FUTURE AHEAD 81

Editorial

SEATTLE, WA – February, 1st, 2022. Let's kick off this months issue by talking about the effect of quantum supremacy as it relates to cybercrime. If you've been following the past several issues of Crypto News, you've read the dozens of articles highlighting the current and future potential positive uses of quantum computers. However, it is said, that there can be no light without the dark. We've seen with other innovations that there's always sinister uses of them by those willing to exploit them. Take a look at article #5 to read more about whether quantum computers will be able to help in the on-going battle with cybercrime or if they will make the problem worse. For those working in the U.S. federal space, take a look at article #29. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has updated its list of exploited vulnerabilities which includes "ancient bugs" as old as from 2013. Even if you're not in the federal space, go ahead and read the article to learn how to reduce your organizations exposure to cyber risks. In the mood to learn something new? Then head towards the end of the newsletter to article #35 and learn about homomorphic encryption. It may give you the solution you've been looking for to meet your regulatory requirements while simultaneously providing broader access to your company's data. Imagine the possibility of searching, analyzing, evaluating, etc. data while not decrypting the information. Now if that's not impressive then I don't know what is. As with every Cyrpto News issue, this months newsletter is a treasure trove of articles that you won't want to miss. Happy reading!

Crypto News is authored by Dhananjoy Dey with this editorial provided by Mehak Kalsi. Both are active members of the Cloud Security Alliance (CSA) Quantum-Safe Security Working Group (QSS WG). The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data.

Disclaimer. The QSS WG does not express an opinion on the validity of the ideas and the claims presented in the articles in this newsletter.

1.IBM Unveils 127-Qubit Quantum Computer

by Steven Leibson
https://www.eejournal.com/article/ibm-unveils-127-qubit-quantum-computer/

On November 16, during its online Quantum Summit, IBM announced that it had successfully completed initial development of the **127-qubit (quantum bit) Eagle quantum computer**. Last year, IBM's Hummingbird quantum computer handled 65 qubits, and, the year before that, the company's Falcon quantum computer was handling calculations using 27 qubits. So the company has been steadily increasing the number of qubits that its quantum machines can handle, roughly doubling the number of operational qubits in its quantum machines on an annual basis. However, the Eagle quantum computer is the last member of IBM's Quantum System One family. Designs have reached the limit of the cryogenic refrigerator used to cool the Josephson Junctions that hold the qubits, so IBM has had to work with Bluefors Cryogenics to develop a new, larger cryogenic platform for bigger machines.

So IBM's announcement of the Eagle computing hardware is a big deal. An Eagle quantum computer can deal with system models in 2^{127} states simultaneously. That's such a large number of states that the Eagle quantum computer cannot be simulated using common digital computers, unlike most previous generations of simpler IBM quantum computers. No more quantum simulators. We're in a whole new world where only quantum computers can run these quantum calculations. Next year, IBM plans to make its 433-qubit Osprey quantum computer operational, and, the following year, it expects the 1121-qubit computer to be operational.

These avian-named quantum computers are not mere science projects for IBM. The company is putting these machines on the cloud and into institutions such as the University of Tokyo, the Cleveland Clinic, and South Korea's Yonsei University, among others, for research. In all, IBM has installed 50 or so first-generation quantum computers around the world.

Building an army of quantum programmers

These quantum computing installations are a farsighted plan by IBM to nurture an army of people versed in programming quantum computers, which is currently an arcane art. Programming for quantum computing is very much at the crawling stage for now, although IBM has developed tools with high-level abstractions to make programming more familiar to computer scientists.

At their heart, quantum computers are fundamentally different from digital computers. Quantum computer scientists seem to have intentionally obscured what is actually going on. During IBM's Quantum Summit in November, there was much talk about quantum gates and circuits. Before I dug into some Google searching, I thought the gates and circuits bore some physical resemblance to electronic gates and circuits.

.

.

.

IBM's chief quantum development tool is called Qiskit, an open-source SDK for working with quantum computers at the level of pulses, circuits, and application modules. As of now, all of IBM's quantum computers to date can be programmed with Qiskit, and the company has developed substantial courses to train people in its use, much as the company once had to train people to program digital computers back in the mid-20th century.

IBM does not envision that you will soon have a quantum computer on or under your desk, and quantum computers will likely always depend on conventional digital computers for input and output. There needs to be some sort of interface between the quantum world and the world of classical physics. Digital computers seem destined for this job. Instead, IBM sees quantum computers as essential data center accelerators, to be used for solving very difficult problems as diverse as drug discovery, computational chemistry, particle physics, fluid dynamics, machine learning, and logistics optimizations.

The cryogenics required for IBM's approach to quantum computing means these beasts will likely be restricted to data centers. But just as computers evolved from mainframes to desktops, to laptops, to pocketable phones, no one knows what a quantum computer will look like in 50 years.

2.Department of Space Demonstrates Entanglement Based Quantum Communication Over 300M Free Space Along With Real Time Cryptographic Applications

by ISRO
https://www.isro.gov.in/update/31-jan-2022/department-of-space-demonstrates-entanglement-based-quantum-communication-over#block-md-megamenu-1

On 27 January 2022, scientists from the two premier laboratories of Department of Space (DOS), viz. Space Applications Centre (SAC) and Physical Research Laboratory (PRL), both from the city of Ahmedabad, have jointly demonstrated quantum entanglement based real time Quantum Key Distribution (QKD) over 300m atmospheric channel along with quantum-secure text, image transmission and quantum-assisted two-way video calling. The demonstration was conducted at SAC, Ahmedabad, between two buildings separated by a distance of 300 m. This experiment and demonstration were repeated over several nights to ensure the repeatability and robustness of indigenously developed QKD system capable of seamlessly generating and utilizing secure keys for various applications.

Shri. S. Somanath, Chairman, ISRO / Secretary, DOS has witnessed this live breakthrough demonstration at SAC, Ahmedabad. Shri. Nilesh M Desai, Director SAC and Dr. Anil Bhardwaj, Director PRL were also present during the demonstration. Various images were encrypted using generated quantum key and transmitted over classical channel from one building to another building separated by 300m and decrypted at the receiving terminal in real time.

This is yet another significant step towards the development of the planned Satellite Based Quantum Communication (SBQC). This feat comes after the earlier breakthrough demonstration of quantum secure videoconferencing by SAC-ISRO using 'prepare-and-measure' quantum communication technology, in free space, over a distance of 300 m on 19 March 2021.

In order to achieve this technology feat, scientists developed various key technologies like robust & high brightness entangled photon source (EPS), BBM92 protocol implementation, NavIC enabled synchronization, polarization compensation technique etc. A cryptographic application software suite with integrated quantum security has also been developed and demonstrated for text, image, video encryption/decryption.

The BBM92 protocol based quantum communication link was demonstrated in the experiment. The secure-key-rate achieved was ~1.8 kbps, with Quantum Bit Error Rate (QBER) of less than 10%. Quantum entanglement was achieved with Bell's parameter and quantum visibility greater than 2.2 and 80% respectively.

With these developments, ISRO, Department of Space is getting ready for satellite based demonstrations of fundamental quantum mechanics experiments as well as quantum communication for future-proof data security.

3.Quantum Computing Threatens Everything — Could It Be Worse Than The Apocalypse?

by Justin Malonson
https://www.entrepreneur.com/article/404091

What is a quantum computer?

A quantum computer is a machine that uses the laws of quantum theory to solve problems made harder by Moore's law (the number of transistors in a dense integrated circuit doubles about every two years). One example is factoring large numbers. Traditional computers are limited to logical circuits with several tens of transistors, while the number of transistors in a quantum processor may be on the order of one to two million. Meaning, these computers will have exponential power, solving problems that traditional computation can't even identify or create solutions for.

The dangers of a quantum computer

In the near future, quantum computers will be so advanced that they will have the capability to simulate very complicated systems. This could be used for simulations in physics, aerospace engineering, cybersecurity and much more. However, once this computer is built, it has the potential to unravel data encryption protocols. It could also potentially compromise air gaps due to its ability to scan vast distances for nearby networked devices or applications that are open. This means that it can become even simpler for external hackers. They may already have access to your computer or computer system via other avenues, like vulnerabilities in web browsers. They could find it much easier because you're not locking up all the doors.

Quantum computers point to a radically new understanding of computing. An understanding that could eventually be used to unlock problems now thought completely intractable. For now, the field seems ripe with potential. Scientists working on quantum computing call it one of the most interesting theoretical tools in artificial intelligence. Think of it as an incredibly powerful calculator programmed with deep domain expertise. Quantum computers promise answers to all sorts of mathematical, scientific and medical questions humans would never have the guts to tackle otherwise. They promise profound breakthroughs in imaging that will rival even experimental intracellular MRI scans; they may help crack wide-ranging databases that are currently unbreakable or they might pick up scant details like geological signatures warning us about tsunamis long before they happen.

Can quantum computers be reprogrammed?

Quantum computers can theoretically be programmed to solve any complex computational problem. But, the act of programming the computer is so expensive and inflexible that someone would need to program it with all possible solutions. Quantum computers threaten everything. The worst part is that security experts can't ever say for sure what you can do to protect against their programming capabilities. They do know, however, that it's possible to reprogram them just as we would with a normal computer. It's just that the task is so complex and difficult that programming would be such a high-level security risk, it might as well never exist.

What does this all mean? It means we need to develop some sort of encryption technology on our smaller devices so not even those who hold all the world's data can see or access it. Quantum computers work differently than traditional computers. That gives the maker of a quantum computer more control than with a conventional computer. They can do things like reverse time and process large data with greater speed. The manufacturer will program the machine before release, which also comes with certain risks. If they change their mind and reprogram it per client needs, they put themselves at risk for security breaches. The catch is that the cryptography keys are only secure if you keep them secret. The slightest leak — say a pinhole camera across the table from something like a quantum computer or a phone call or email intercepted while being decrypted — would enable an adversary to not just unscramble your message but steal your keys. The threat made by quantum computing has been speculated since before it was even technologically feasible to build a quantum computer. But now that we're nearly there, the situation might be even more dire than you can imagine.

Current safety standards

As quantum computers allow for more efficient algorithms, the dangers of hacking increase. Such security risks have been a top priority at Google. They have high expectations for what approach they will take to create their future quantum machine. In the meantime, DARPA (Defense Advanced Research Projects Agency) has set out grand challenges for computer science with a hefty $2 million prize. DARPA's goal is to keep U.S. cyber strength relevant amid the rapid decline in Moore's Law and potential loss of global technological leadership. If quantum computers proliferate, they will threaten everything — not just bank records and medical documents, but everything. They represent a security leak so fundamental that it could be worse than the apocalypse. The quantum computer poses a possible threat to the infrastructure of the United States. Yet the American authorities do not have enough measures in place to stop this type of danger. One way that they can defend themselves is by inventing new safety standards that work with the current technologies.

Whenever quantum computing matures, however, it will present a vigorous challenge. Computer scientists will need to develop the protocols and protections necessary to ensure security for this emerging technology. If these precautions are not taken, quantum computing could lead to disastrous outcomes in cyber security. There needs to be a protocol developed to provide security for quantum computers. Hackers will be able to access and disrupt live systems, which calls for an urgent need of advancements in cyber security. These new systems can't just implement existing protection protocols because they're not fully developed yet. The cost of research and development is high and the profits once the product is finished are relatively low.

Quantum computing is a hot topic at this moment in time that will impact society in a way we can't even predict if we don't acknowledge its significance now. Most computers today work in accordance with digital signals. If someone tries to hack the computer, it will change that digital signal into another form or cancel it out, which can be easily noticed. However, quantum computers use quantum bits for calculations. They are tied together in a way that makes them so sensitive to changes in information that they are exponentially more vulnerable to hacks than digital computers. If someone manages to hack a quantum computer — though not yet possible — it would have serious implications for maintaining our safety standards.

How can companies protect themselves from the threat of quantum computers?

If the leaked NSA documents are to be believed, then we may be in for a rude awakening when quantum computers become technologically feasible. These machines will be able to perform calculations in far less time than any conventional computer and render our current encryptions ineffectual. The leaks claim that in 30 years, two medium-sized quantum computers would be able to even break the security of RSA (cryptosystem) — which is currently set at 2048 bits.

Any business that relies on modern cryptography is at risk of being hacked in the near future. But what can companies do to protect themselves? As it turns out, there are some pretty straightforward solutions which firms can preserve (or improve) security amid all this hullabaloo with quantum computing. The authors recommend investing in encryption techniques like Bitcoin, the blockchain and the TLS.

In simple terms, quantum computers process information differently from today's digital computers. This is because of their ability to have bits which sit in more than one state simultaneously, meaning they can perform many calculations at a time. In a future dominated by quantum computing, all regular computing will be made virtually obsolete. Hackers will be able to access the deepest secrets of companies without needing a password. To avoid this fate, companies need to embrace encryption techniques that guard against quantum technology, but they cannot afford to stop innovating too drastically.

The looming potential threat of quantum computing should be taken seriously, but this doesn't mean you should panic. The best way to protect yourself is to plan ahead and think about possible solutions. Incorporating elements of quantum cryptography may not always be possible for every client because of the cost. But, it could help secure an important client who cannot risk future interference in their sensitive operations.

4.Why Gate-Level Quantum Design Is Becoming Impossible

by Amir Naveh
https://thequantuminsider.com/2022/01/27/why-gate-level-quantum-design-is-becoming-impossible/

Today, most quantum software is written at the gate level, performed by specifying the interconnection between qubits and quantum gates.

But as quantum computers become more powerful and complex – reaching 100's or 1000's of qubits very soon – it will become nearly impossible to write valuable and sophisticated quantum code this way.

Here are seven examples of why this is the case:

- **Reusing auxiliary qubits**. Auxiliary qubits (sometimes called ancillary qubits or ancilla) often need to be allocated and de-allocated. But once an auxiliary qubit has been used, the designer can reuse it down the circuit. This reuse is either to make specific calculations more efficient or to ensure that quantum circuits are reversible. Keeping track of which qubits are auxiliary and can be reused becomes increasingly difficult as the number of qubits increases.

- **Un-computation strategy**. Un-Computation is useful in quantum software when trying to free auxiliary qubits for future use or to disentangle some of the qubits to reduce noise. We can also uncompute intermediate results when the result is no longer needed in the algorithm. In many cases, the question of when and if a function should be uncomputed is complex. For example, in quantum arithmetic, we can uncompute the intermediate results in many different ways, trading off the qubits needed and the circuit depth.

- **Multiple function implementations**. The user may wish to perform some function, e.g. a quantum adder, an mcmt gate, a state preparation, etc. These functions have diffent implementations, trading off complexity, accuracy, the number of qubits, and the resources needed. As a simple example, mcmt gates can be implemented in many ways by choosing the number of available auxiliary qubits. Choosing which function instance to use at each stage is a complex problem that cannot be done manually for large circuits.

- **Organizing the Hamiltonian terms in the right order**. In some cases, we encode Hamiltonians of a certain system into the quantum circuit. This is common for example in the QAOA framework. A common approach is Trotterization, where the Hamiltonian is broken into local terms which are placed individually. Placing these different terms has many different options. Naively, a Hamiltonian with n local terms has n! possible placement options. Placing these local terms manually will give a much longer (larger circuit depth) than necessary.

- **Trading off depth, number of qubits, and accuracy at the circuit level.**

  We have many design choices, some of which were discussed above. We are faced with global constraints on the circuit – number of available qubits, total coherence time, gate fidelities, hardware connectivity, native gates, etc. We also wish to optimize the circuits under the constraints, for example, achieve maximal accuracy, minimize the number of T gates, etc. Optimizing under the given constraints at the circuit level requires knowledge of all the different design possibilities, as well as large computational power to go over the countless design choices.

  - ✦ **Optimizing functions for specific hardware**. There are many different hardware implementations of quantum computers. They differ in the number of qubits, their noise characteristics, the type of native gates, the connectivity between qubits, and much more. As a result, code that is optimized for one hardware may be far from optimal for another. The ability to understand the hardware characteristics and define them as constraints that need to be satisfied is particularly important during this market period when the pace of innovation is fast and the number of different architectures is large.

  - ✦ **Analyzing the circuit at the functional level**. When one wishes to debug a circuit or modify a circuit created by someone else, it is often good to start at a high level. But how can you start at a high level when working at the gate level? Using a classical analogy, it is much easier to dive from Python code to assembly language than try to deduce the Python intent by looking at the assembly language code.

This evolution mirrors what we have seen in other industries. Very few people write assembly-language code for high-end CPUs, and even fewer build manual 'netlist' files for electronic circuits. The process of climbing up the abstraction stack is common and probably unavoidable in many cases, including quantum computing.

So the choice is yours: continue to work at the gate level, or start adopting the platforms and skills that allow you to code that for larger computers as well.

5.Will Quantum Computing Help or Hinder The Fight Against Cybercrime?

by Lara Williams

https://www.investmentmonitor.ai/tech/quantum-computing-cyber-security-crime

Quantum supremacy is the inflection point at which quantum computing will outpace the speed and accuracy of classical computing. Analyst GlobalData predicts a time frame of about five years, but forecasts vary wildly, and many come with caveats around whether use cases and standards will align with quantum technology development.

With quantum supremacy, every organisation in the world that stores and processes data will be wide open to a cyberattack. Hyperbole? Not so, according to Google CEO Sundar Pichar, who has said publicly that in five to ten years, quantum computers will break the encryption systems we use today. Perhaps most concerning is that data sent today can be retroactively decrypted in so-called "hack now, decrypt later" attacks. If this scenario is accurate, large organsiations are facing a ticking time bomb if action is not taken immediately to mitigate future risk.

Ransomware attacks increased 151% in 2021, according to the World Economic Forum, with an average of 270 cyberattacks per organisation, a 31% increase from 2020. While these attacks are damaging (each breach costing about $3.6m), the data amassed in these security breaches could have even bigger consequences down the line.

Quantum's concentration on security

There has been a preoccupation with security and quantum computing for a long time, according to Quantinuum (formerly Cambridge Quantum) CEO Ilyas Khan. "Quantum computers will render pretty useless most existing methods of encryption, and, in fact, even the newer, more quantum-resistant methods are frankly untested," he says.

Cybersecurity has increasingly become a boardroom topic and business leaders are more aware of the threat to their businesses, both financial and reputational.

Khan notes that governments and large organisations have historically viewed quantum computing through the lens of this growing cyber threat. In addition to this, the rise of ever more sophisticated nation state-sponsored attacks such as the 2020 Solar Winds global supply chain attack, which swept through the US federal government, and the May 2021 Colonial Pipeline hack, which took down parts of the US critical national infrastructure, demonstrate the vulnerability of existing technology platforms and serve as a stark warning of the potential catastrophic damage from quantum attacks.

However, Khan believes quantum technology is not simply a threat, and that it also presents a solution. "Quantum computing provides a defence for anything out there that is a classical computing threat to security as well as a defence for future attacks by quantum computers," he says.

Data is currently protected by encryption based on the RSA and AES algorithms. In simple terms, cybersecurity is determined by randomly generated cryptographic keys. The quality of these keys is measurable by their randomness. Classical methods of encryption are broken by hackers when keys have poor randomness. Because the RSA and AES standards are not truly random, they have been shown to be breakable. The unbreakable nature of quantum keys is a function of the unpredictable behaviour that lies at the very heart of quantum mechanics. Post-quantum algorithms for key generation are currently in the process of being standardised by the US National Institute of Standards and Technology (NIST) and are expected to become codified any time between 2022 and 2024.

How can quantum computing fight cybercrime?

GlobalData's thematic research, published in February 2021, says any predictions about quantum computing's future market size are educated guesses at best given its nascence and the prospect of unanticipated breakthroughs. Market size in 2020 was said to be between $80m and $500m, rising to anywhere between $1bn and $5bn by 2025. GlobalData principal analyst David Bicknell says quantum security will be a significant driver of investment into the sector.

The classical computing cybersecurity sub-sector is growing rapidly, and GlobalData's 2022 technology predictions deemed cybersecurity a primary business theme for the coming year. The analyst forecasts that the global cybersecurity market will grow to $238bn by 2030, up from $115bn in 2020.

Given that quantum computing cybersecurity solutions can be integrated with classical computing architectures, the market opportunity for the quantum cybersecurity market is broader than it appears at first glance.

Quantinuum's security product, Quantum Origin, for example, can be integrated into existing cybersecurity systems to mitigate classical computing cyber threats as well as future proofing for the quantum age. Quantinuum head of cybersecurity Duncan Jones says it is important that the company's customers don't feel they need advanced physics degrees to understand quantum cybersecurity products.

Quantinuum's cloud-based product delivers cryptocraphic keys that have been verified from a quantum source that can easily be integrated with existing hardware security modules and systems – supporting traditional algorithms, such as RSA or AES, as well as post-quantum cryptography algorithms.

It will take time for businesses to migrate to quantum-safe architectures and Jones believes businesses are underestimating how much work will be required to become quantum resistant. "Estimates of when the cyber threat of quantum will arrive vary, but there is a universal consensus that the time to act is now," says Jones.

For some business areas, Jones says it is already too late. For example, the internet of things (IoT) and digital manufacturing are areas particularly vulnerable to the quantum threat. "IoT devices are low-power devices, they don't have access to many good sources of randomness," he says. "I think we are definitely going to see businesses that have not moved early enough, and in five to ten years' time, or whenever it is that they are genuinely threatened, they will wish they had move a lot faster," he adds.

This is a sentiment echoed by Bicknell, who urges companies to take action. "Developing, testing, deploying and improving new quantum-safe cryptographic solutions will require years of research and design by different stakeholders. There is no time to be lost," he says.

Early adopters such as IT infrastructure company Fijitsu are testing quantum-enhanced keys alongside traditional algorithms. Dr Houshan Housmand, chief technology officer research lead at Fijitsu, says the current trend of moving from a data centre model towards a cloud model will require security enhancements for resilience against quantum attacks. "This is a major concern for us," he adds.

Housmand points out that the company's security concerns are echoed by the UK's National Cyber Security Centre (NCSC) in terms of the need for quantum random number generators, with particular research emphasis on integration challenges with large systems.

However, while the NCSC's November 2020 white paper on quantum cybersecurity recommends that large organisations should factor the threat of quantum computer attacks into their long-term road maps, it also cautions against early adoption of non-standardised quantum-safe cryptography, "given the current lack of clarity around which variants will offer the best balance of security and performance, and which specific parameter sets to use". The paper goes on to warn that "unnecessary haste and over-reliance on new approaches to cryptography may introduce costly security weaknesses".

The NCSC expects that major commercial products and services will transition to quantum-safe cryptography once NIST standards become available between 2022 and 2024. The government body therefore recommends that the majority of users follow normal cybersecurity best practice and wait for the development of standards-compliant quantum-safe cryptographic products.

Once industry standards are agreed, the market for quantum cybersecurity products is likely to develop rapidly. A consumer market is also expected to grow, with Samsung already having launched its Galaxy Quantum2 smartphone with an inbuilt quantum random number generator chip developed by Swiss quantum security company ID Quantique.

For now, the quantum computing industry's attention is keenly focused on the much-anticipated NIST standards for quantum-safe cryptography. Once this milestone is reached, the quantum cybersecurity industry is likely to see an inflection point whether or not quantum supremacy has arrived.

6.How Big Does Your Quantum Computer Need to Be?

by American Institute of Physics
https://phys.org/news/2022-01-big-quantum.html

Quantum computers are expected to be disruptive and potentially impact many industry sectors. So researchers in the United Kingdom and the Netherlands decided to explore two very different quantum problems: breaking the encryption of Bitcoin (a digital currency) and simulating the molecule responsible for biological nitrogen fixation.

In AVS Quantum Science, the researchers describe a tool they created to determine how big a quantum computer needs to be to solve problems like these and how long it will take.

"The majority of existing work within this realm focuses on a particular hardware platform, superconducting devices, like those IBM and Google are working toward," said Mark Webber, of the University of Sussex. "Different hardware platforms will vary greatly on key hardware specifications, such as the rate of operations and the quality of control on the qubits (quantum bits)."

Many of the most promising quantum advantage use cases will require an error-corrected quantum computer. Error correction enables running longer algorithms by compensating for inherent errors inside the quantum computer, but it comes at the cost of more physical qubits.

Pulling nitrogen out of the air to make ammonia for fertilizers is extremely energy-intensive, and improvements to the process could impact both world food scarcity and the climate crisis. Simulation of relevant molecules is currently beyond the abilities of even the world's fastest supercomputers but should be within the reach of next-gen quantum computers.

"Our tool automates the calculation of the error-correction overhead as a function of key hardware specifications," Webber said. "To make the quantum algorithm run faster, we can perform more operations in parallel by adding more physical qubits. We introduce extra qubits as needed to reach the desired runtime, which is critically dependent on the rate of operations at the physical hardware level."

Most quantum computing hardware platforms are limited, because only qubits right next to each other can interact directly. In other platforms, such as some trapped ion designs, the qubits are not in fixed positions and can instead be physically moved around—meaning each qubit can interact directly with a wide set of other qubits.

"We explored how to best take advantage of this ability to connect distant qubits, with the aim of solving problems in less time with fewer qubits," said Webber. "We must continue to tailor the error-correction strategies to exploit the strengths of the underlying hardware, which may allow us to solve highly impactful problems with a smaller-size quantum computer than had previously been assumed."

Quantum computers are exponentially more powerful at breaking many encryption techniques than classical computers. The world uses RSA encryption for most of its secure communication. RSA encryption and the one Bitcoin uses (elliptic curve digital signature algorithm) will one day be vulnerable to a quantum computing attack, but today, even the largest supercomputer could never pose a serious threat.

The researchers estimated the size a quantum computer needs to be to break the encryption of the Bitcoin network within the small window of time it would actually pose a threat to do so—in between its announcement and integration into the blockchain. The greater the fee paid on the transaction, the shorter this window will be, but it likely ranges from minutes to hours.

"State-of-the-art quantum computers today only have 50-100 qubits," said Webber. "Our estimated requirement of 30 [million] to 300 million physical qubits suggests Bitcoin should be considered safe from a quantum attack for now, but devices of this size are generally considered achievable, and future advancements may bring the requirements down further.

"The Bitcoin network could perform a 'hard-fork' onto a quantum-secure encryption technique, but this may result in network scaling issues due to an increased memory requirement."

The researchers emphasize the rate of improvement of both quantum algorithms and error- correction protocols.

"Four years ago, we estimated a trapped ion device would need a billion physical qubits to break RSA encryption, requiring a device with an area of 100-by-100 square meters," said Webber. "Now, with improvements across the board, this could see a dramatic reduction to an area of just 2.5-by-2.5 square meters."

A large-scale error-corrected quantum computer should be able to solve important problems classical computers cannot.

"Simulating molecules has applications for energy efficiency, batteries, improved catalysts, new materials, and the development of new medicines," said Webber. "Further applications exist across the board—including for finance, big data analysis, fluid flow for airplane designs, and logistical optimizations."

7.A New Language For Quantum Computing

by Rachel Gordon
https://news.mit.edu/2022/new-language-quantum-computing-twist-0124

Time crystals. Microwaves. Diamonds. What do these three disparate things have in common?

Quantum computing. Unlike traditional computers that use bits, quantum computers use qubits to encode information as zeros or ones, or both at the same time. Coupled with a cocktail of forces from quantum physics, these refrigerator-sized machines can process a whole lot of information — but they're far from flawless. Just like our regular computers, we need to have the right programming languages to properly compute on quantum computers.

Programming quantum computers requires awareness of something called "entanglement," a computational multiplier for qubits of sorts, which translates to a lot of power. When two qubits are entangled, actions on one qubit can change the value of the other, even when they are physically separated, giving rise to Einstein's characterization of "spooky action at a distance." But that potency is equal parts a source of weakness. When programming, discarding one qubit without being mindful of its entanglement with another qubit can destroy the data stored in the other, jeopardizing the correctness of the program.

Scientists from MIT's Computer Science and Artificial Intelligence (CSAIL) aimed to do some unraveling by creating their own programming language for quantum computing called Twist. Twist can describe and verify which pieces of data are entangled in a quantum program, through a language a classical programmer can understand. The language uses a concept called purity, which enforces the absence of entanglement and results in more intuitive programs, with ideally fewer bugs. For example, a programmer can use Twist to say that the temporary data generated as garbage by a program is not entangled with the program's answer, making it safe to throw away.

While the nascent field can feel a little flashy and futuristic, with images of mammoth wiry gold machines coming to mind, quantum computers have potential for computational breakthroughs in classically unsolvable tasks, like cryptographic and communication protocols, search, and computational physics and chemistry. One of the key challenges in computational sciences is dealing with the complexity of the problem and the amount of computation needed. Whereas a classical digital computer would need a very large exponential number of bits to be able to process such a simulation, a quantum computer could do it, potentially, using a very small number of qubits — if the right programs are there.

"Our language Twist allows a developer to write safer quantum programs by explicitly stating when a qubit must not be entangled with another," says Charles Yuan, an MIT PhD student in electrical engineering and computer science and the lead author on a new paper about Twist. "Because understanding quantum programs requires understanding entanglement, we hope that Twist paves the way to languages that make the unique challenges of quantum computing more accessible to programmers."

Yuan wrote the paper alongside Chris McNally, a PhD student in electrical engineering and computer science who is affiliated with the MIT Research Laboratory of Electronics, as well as MIT Assistant Professor Michael Carbin. They presented the research at last week's 2022 Symposium on Principles of Programming conference in Philadelphia.

Untangling quantum entanglement

Imagine a wooden box that has a thousand cables protruding out from one side. You can pull any cable all the way out of the box, or push it all the way in.

After you do this for a while, the cables form a pattern of bits — zeros and ones — depending on whether they're in or out. This box represents the memory of a classical computer. A program for this computer is a sequence of instructions for when and how to pull on the cables.

Now imagine a second, identical-looking box. This time, you tug on a cable, and see that as it emerges, a couple of other cables are pulled back inside. Clearly, inside the box, these cables are somehow entangled with each other.

The second box is an analogy for a quantum computer, and understanding the meaning of a quantum program requires understanding the entanglement present in its data. But detecting entanglement is not straightforward. You can't see into the wooden box, so the best you can do is try pulling on cables and carefully reason about which are entangled. In the same way, quantum programmers today have to reason about entanglement by hand. This is where the design of Twist helps massage some of those interlaced pieces.

The scientists designed Twist to be expressive enough to write out programs for well-known quantum algorithms and identify bugs in their implementations. To evaluate Twist's design, they modified the programs to introduce some kind of bug that would be relatively subtle for a human programmer to detect, and showed that Twist could automatically identify the bugs and reject the programs.

They also measured how well the programs performed in practice in terms of runtime, which had less than 4 percent overhead over existing quantum programming techniques.

For those wary of quantum's "seedy" reputation in its potential to break encryption systems, Yuan says it's still not very well known to what extent quantum computers will actually be able to reach their performance promises in practice. "There's a lot of research that's going on in post-quantum cryptography, which exists because even quantum computing is not all-powerful. So far, there's a very specific set of applications in which people have developed algorithms and techniques where a quantum computer can outperform classical computers."

An important next step is using Twist to create higher-level quantum programming languages. Most quantum programming languages today still resemble assembly language, stringing together low-level operations, without mindfulness towards things like data types and functions, and what's typical in classical software engineering.

"Quantum computers are error-prone and difficult to program. By introducing and reasoning about the 'purity' of program code, Twist takes a big step towards making quantum programming easier by guaranteeing that the quantum bits in a pure piece of code cannot be altered by bits not in that code," says Fred Chong, the Seymour Goodman Professor of Computer Science at the University of Chicago and chief scientist at Super.tech.

8.Twin-Field Quantum Key Distribution (QKD) Across an 830-Km Fibre

by Thamarasee Jeewandara
https://phys.org/news/2022-01-twin-field-quantum-key-qkd-km.html

By using quantum key distribution (QKD), quantum cryptographers can share information via theoretic secure keys between remote peers through physics-based protocols. The laws of quantum physics dictate that photons carrying signals cannot be amplified or relayed through classical optical methods to maintain quantum security. The resulting transmission loss of the channel can limit its achievable distance to form a huge barrier to build large-scale quantum secure networks. In a new report now published in Nature Photonics, Shuang Wang and a research team in quantum information, cryptology and quantum physics in China developed an experimental QKD system to tolerate a channel loss beyond 140 dB across a secure distance of 833.8 km to set a new record for fiber-based quantum key distribution. Using the optimized four-phase twin-field protocol and high quality setup, they achieved secure key rates that were more than two orders of magnitude greater than previous records across similar distances. The results form a breakthrough to build reliable and terrestrial quantum networks across a scale of 1000 km.

Quantum cryptography and twin-field quantum key distribution (QKD)

Quantum key distribution is based on fundamental laws of physics to distribute secret bits for information-theoretic secure communication, regardless of the unlimited computational power of a potential eavesdropper. The process has attracted widespread attention in the past three decades relative to the development of a global quantum internet, and matured to real-world deployment through optical-fiber networks. Despite this, wider applications of QKD are limited due to channel loss, limiting increase in the key rate and range of QKD. For example, photons are carriers of quantum keys in a QKD setup, and they can be prepared at the single-photon level to be scattered and absorbed by the transmission channel. The photons, however, cannot be amplified, and therefore the receiver can only detect them with very low probability. When transmitted via a direct fiber-based link from the transmitter to the receiver, the key rate can therefore decrease with transmission distance. As a result, twin-field QKD can build a promising rate-distance relationship to overcome limits and achieve a secret key rate across long distances. Researchers have taken great efforts to develop its theory and experimentally demonstrate the unique advantages of the system. Wang et al. analyzed the cumulative results of recent long-distance fiber-based QKD experiments for fiber lengths beyond 450 km, revolving around twin-field quantum key distribution (TF-QKD) protocols to illustrate huge advantages of TF-QKD, while highlighting advances of the present study.

The four-phase twin field quantum key distribution protocol

The protocol contained five steps: At step one, Alice and Bob independently prepared a weak coherent state with randomly chosen intensity and probabilities. In step two, within the code mode, Alice (or Bob) can pick a 'key' bit and a 'basis' bit to randomly prepare a weak coherent state. During step three, Alice and Bob sent their weak coherent states to an untrusted middle station Charlie, who could make the incoming states interfere on a beamsplitter. The experimental setup contained two single-photon detectors located at two distinct outputs of the beam splitter labeled D_0 and D_1, respectively, where Charlie must publicly announce the clicks of D_0 and D_1. The team repeated the first three steps for a number of times (labeled N_{tot}). During step four, among the N_{tot} trials, only when just one of D_0 and D_1 clicks were they retained for further processing. Alice and Bob then broadcast the intensities for each retained trial to ultimately form the sifted key string. Finally, according to resulting lengths, Alice and Bob could share a secret key string with length G, from their sifted key string with a failure probability not larger than a value of $\epsilon_s ec = 2^{-31}$ computed in the study.

The twin-field quantum key distribution (TF-QKD) experimental system

The experimental setup required optical pulses from two remote users to stably interfere in the intermediate station (Charlie). The wavelength difference and phase difference between Alice and Bob's sources were designated to be relatively stable across time. Using a free running common laser, the team locked both Alice's and Bob's sources to reconcile their central wavelength values and employed a time division multiplexing method to compensate for fast phase drift introduced by the fiber channels. These fiber channels included the servo channel to transmit light from the common laser to Alice (or Bob), and the quantum channel adopted to transmit the time-multiplexed signal from Alice and Bob to Charlie. During the experiments, after passing through corresponding quantum channels and polarization compensation modules, Alice's and Bob's encoded twin fields interfered on Charlie's beam splitter for detection by two superconducting nanowire single-photon detectors. During experimental realization, the team formed a high-speed and low-noise TF-QKD system and optimized its performance by reducing the effect of noises originating from the source, channel and the detector. When compared to earlier experiments, a key advantage of the current experiment was its lack of requirements for optical amplifiers inserted to increase the power of classical signals, while reducing the complexity of the setup for scientists to generate remote, high-quality twin fields with reduced complexity and cost.

Generating twin fields—optimizing the setup

Wang et al. reduced the noise from the source and the servo channel to develop a highly sensitive and repeater-like laser source to ultimately generate twin-fields with 10-mw output power. They improved the sensitivity of the repeater-like laser source to work with very weak input power, even as low as 0.2 nW. The resulting twin-fields were generated with very high quality, which they optimized to achieve low multipath interference (MPI) noise, with high interference visibility in the quantum channels. The stability of the twin-field system played an important role to collect enough counts of quantum pulses, for the QKD system to function continuously for several weeks. The longest fiber-length across which Wang et al. could keep a relatively high interference visibility and achieve a positive key rate was 833.80 km, with a secure key rate of 0.014 bps after maximizing the outcome.

Outlook

In this way, Shuang Wang and colleagues showed how a fiber-based quantum key distribution (QKD) could be realized across a distance of 833.8 km with a channel loss of 140 dB. The new setup set records for tolerant channel loss and the long transmission distance of fiber-based QKD, while achieving secure key rates that outperformed previous twin-field quantum key distribution experiments at similar distances. The absence of optical amplifiers in the setup helped reduce the complexity and cost with great potential in field and network applications. The study provides a practical format to extend the transmission distance and pave the way towards a wider-range of QKD experiments.

9.The Biden White House Gets Quantum Right—At Last

by Arthur Herman
https://www.forbes.com/sites/arthurherman/2022/01/21/the-biden-white-house-gets-quantum-right-at-last/?sh=313dc8fb598a

In my last column I predicted that quantum would be one of the three most important and disruptive technologies we'd all be facing in 2022, alongside cryptocurrencies and hypersonics.

Sure enough, barely a week has passed and the White House has confirmed that prediction.

On Wednesday President Biden signed a National Security Memorandum "on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," which will have huge implications for quantum technology and quantum security for the United States and for the world.

This document (NSM-8) is the first I'm aware of coming out of the White House national security apparatus that specifically mentions quantum-resistant cryptography in the context of current federal cybersecurity planning. That's a big victory for the Quantum Alliance Initiative, which has been pushing the quantum security issue for the past four years, and for quantum information science generally. The document instructs the National Security Agency to release to Chief Information Officers any relevant documents relating to "quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary."

The key provision is here:

Within 180 days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI//NOFORN.

These sections of a memorandum devoted to protecting the federal government from cybersecurity attack are a big score for those of us who've been pressing the government to at least adopt a timeline for identifying which agency systems will be vulnerable to a quantum computer attack: which is just about every agency from Treasury and the Pentagon on down.

This has been a major goal we at the Quantum Alliance Initiative at the Hudson Institute have been fighting for we started in 2018, i.e. getting someone in the American national security apparatus to take the quantum computer threat seriously as a cybersecurity priority.

Still, NSM-8 leaves a huge gap in raising awareness of the need to defend against the quantum threat: namely, the private sector.

Given the fact that the federal government finally admits this is a security threat grave enough to demand action from agencies within the next 180 days, that's all the more reason why private industry needs to take this threat seriously as we've been urging in these columns, without waiting for the slow-moving bureaucratic machinery of Washington to put together a plan to protect the rest of us.

That means the private sector, especially our biggest companies and our highly vulnerable financial sector, need to make plans to take on the quantum threat at least as systematically as the federal government now does, and to be ready well before 2030, when the threat of large-scale quantum computers starts to become real.

But there's more that NSM-8 doesn't explain.

The first is that there are right now safe ways to protect data and networks from future quantum intrusion but also existing cyber attackers and hackers, using quantum resistant cryptography that private companies in the United States and Canada have developed and deployed. There's no reason to wait until the NSA or the National Institute of Standards and Technology (NIST) make their final selection of quantum-resistant algorithms, and federal agencies finally respond.

In addition, there are companies here in the U.S. and other countries that are already providing customers with quantum-based cryptographic solutions such quantum key distribution (QKD) for protecting vital communications and links, which are particularly appropriate for certain systems, e.g. industrial systems like SCADA and the power grid—and again which protect users from current cyber threats as well as future quantum threats.

Finally, getting us quantum-ready and quantum-secure needs to be an international effort, involving partners in Europe, Asia, and the Middle East to develop and deploy quantum-safe solutions. Otherwise, what we'll discover well before 2030 is that a single U.S. ally whose government or corporations aren't ready to face a quantum computer attack puts us all at risk—a risk that borders on the catastrophic.

All the same, NSM-8 is a landmark document and the Biden administration deserves praise for releasing it. Consider it a long-awaited wake-up call for understanding how important quantum technology is going to be for our country, and for the world. Our major quantum computer companies like IBM and Google and Microsoft, now also need to embrace the importance of quantum readiness, since their future is as much as at stake as the rest of us.

We all have to make sure that quantum information science, including computing and networking, is able to advance without causing major disruptions in our national security, our lives, or the prospects of freedom around the world.

10.Research Demonstrates A New Technique For Improving Long-Distance Quantum Key Distribution in A Real-World Field

by INRIM - Istituto Nazionale di Ricerca Metrologia
https://phys.org/news/2022-01-technique-long-distance-quantum-key-real-world.html

An experiment, performed by Istituto Nazionale di Ricerca Metrologica (INRIM) on 200 km of the Italian Quantum Backbone, in collaboration with Toshiba Europe, shows that coherent laser interferometry considerably improves the performances of quantum key distribution protocols in long-distance, real-world networks. The study has been published in Nature Communications.

Quantum Key Distribution (QKD) protocols enable cryptographic keys to be shared between distant parties with an intrinsic security guaranteed by the laws of quantum mechanics. This is made possible by the transmission of single photons, the elementary particles of which light is made of.

The interest for this subject extends well beyond the scientific community, and has now a strong strategic and commercial relevance. The European Commission, within the "European Quantum Communication Infrastructure" intitative, aims at integrating quantum key distribution technologies into specific services throughout the European Union within the next 10 years, and INRIM will take part in the design of this infrastructure with the OQTAVO project.

One of the main obstacles towards the realization of a long-reach quantum network is the "fragility" of quantum signals: Single-photon states carry an extremely low energy, which makes them hardly detectable, even moreso considering that 99% is lost after traveling 100 km via telecommunication optical fibers. In addition, the information carried by the remaining single-photon states is severely distorted.

INRIM has already investigated these problems in a metrological context, and has developed, in collaboration with other NMIs, specific laser interferometry techniques that allow recovering the information which is transmitted through long-distance optical fiber. Nowadays, these techniques are at the core of state-of-the-art atomic clock comparisons.

Now, with a synergistic exploitation of coherent laser interferometry, single-photon technologies and quantum metrology, INRIM shows that the information contained in single photon states can be significantly improved, allowing lower error rates and increasing the length of exchanged messages. These improvements pave the way for more efficient QKD protocols exploiting the twin-field quantum key distribution technique, which is currently seen as the most promising candidate for long-reach quantum networks.

The experiment was conducted along a 200-km span of the Italian Quantum Backbone, an 1800-km infrastructure developed by INRiM for the atomic time and frequency distribution to research facilities and high-tech companies in Italy and science applications in fundamental physics, geophysical remote sensing, and quantum technologies.

This study is also the result of a collaboration with Toshiba Europe, leading company in the development of commercial quantum technology products, and the network provider TOP-IX Consortium, active throughout northern Italy, which dedicated part of its infrastructure to this research.

This synergy enabled the researchers to achieve an outstanding result on the road to developing a European quantum communication infrastructure.

11.The Race For Quantum-Resistant Cryptography

by Heidi Vella
https://eandt.theiet.org/content/articles/2022/01/the-race-for-quantum-resistant-cryptography/

That large-scale universal quantum computers could break widely used encryption methods is well known, but what was once seen as a distant, even theoretical, problem is now driving the latest technology race.

There isn't yet a universal quantum computer big enough to break the widely used public key encryption systems, such as RSA, that secure everyday online information exchanges. Nor does anyone know when there will be. But with many predicting a significant breakthrough this decade, companies and governments are racing to launch cryptographic solutions so they can claim a stake in what is expected to be a billion-dollar market.

Public key encryption is based on the assumption that factoring integers – whole numbers – with several hundred or more digits is practically impossible. An algorithm known as Shor showed that a quantum computer could meet the challenge, however, allowing bad actors to decrypt information and spy on communications without detection. And they wouldn't even need a phishing email to do it. What's more, governments are increasingly concerned about the risk of '**harvest and decrypt later attacks**', whereby an adversary steals sensitive information to decode when they have the quantum capability.

Yet developing cryptographic defences for a threat that has not yet materialised and uses information belonging to a notoriously mind-blowing realm of physics is no mean feat. Most advanced quantum cryptography efforts, such as random number generation (RNG) and quantum key distribution (QKD), still have technological limitations. But there's no doubt the field is experiencing its most exciting decade yet, with commercial quantum cryptography solutions now emerging.

UK-based Arqit is an interesting example. The firm, started by David Williams, a former investment banker and founder of telecom satellite company Avanti, has garnered much debate within quantum crypto circles for its somewhat opaque solution that uses neither QKD nor RNG.

The firm says it has invented a new, **patented quantum protocol called Arc19 powered by satellites**, which are set to launch in 2023. Its technology is a downloadable-to-any-device platform-as-a-service called 'QuantumCloud' that will initially be used for quantum-resistant communication between defence aircraft and drones and control centres, as well as blockchain, but could also work for Internet of Things (IoT) and smart city applications. Arqit has already signed a flurry of deals with major firms such as Babcock, BT, Verizon, and Northrop Grumman, as well as "large government customers globally", which it says it can't talk about.

According to its founder, the satellites send information encoded into the quantum properties of photons, which the laws of physics determine can never be stolen, to data centres on Earth.

When one device wants to create a key with another, they both use their architect software to talk to different data centres to access an identical set of random numbers. Using these, they can create a brand new shared random number and ephemeral key to communicate securely. Keys can be created infinitely and work inside a pre-existing algorithm called AES256 (The Advanced Encryption Standard), which the US National Security Agency already recommends as 'safe' against attacks by a large quantum computer because it uses a sufficiently large key.

The simplicity of the technology can "seamlessly make the world secure", according to Williams. "Although our tech stack contains transformational deep technological innovation, and our software protocol endpoints are completely new, we're injecting keys into an algorithm that you already have installed on all of your devices – no revolution required," he adds.

Arqit describe the system as "trustless" because the keys are never created by a third party; not even the satellites know what they are. This solves a fundamental problem with QKD satellite protocols: that data can be sent either globally or trustlessly, but not both, says Williams.

"Anyone who is trying to build a system that does QKD by satellite is wasting their time; it doesn't work. If you can't send keys globally, you're of no interest to the internet. If you can't send keys trustlessly, you're not secure," explains Williams. "No one has ever devised a cryptographic system which can make endless computationally secure, trustless and ephemeral keys. That is a world first."

Rhys Lewis, head of the Quantum Metrology Institute at the National Physical Laboratory, doesn't agree with the first point, however: "QKD over satellite removes the need for trusted nodes as the signal can be picked up from one point and transmitted directly to the receiving station. Only the satellite must be trusted," he explains.

QKD by satellite is a key area of research and development, as it's thought it can help overcome some of the range problems experienced by QKD via optical fibre. The UK and Singapore have a £10m initiative to co-develop QKD Qubesat, a satellite based on the CubeSat standard that will use a pioneering QKD technology to test the secure distribution of cryptographic keys over globe-spanning distances.

QKD protocols provide a mechanism for two remote parties to agree a shared secret key, where the key cannot be observed or tampered with by an adversary without alerting the original parties.

Last year, industry leader Toshiba launched the fruits of 20 years of research into development of QKD over optical fibre. Its commercial hardware and management software combines RNG and PQC (Post-Quantum Cryptography) technologies for an all-in-one package that Toshiba will use to build the world's first commercially available quantum-secured metro network with BT. The network will connect the London financial and creative industries with data centres to the west of the city. It's expected to be operational in early 2022. Previously the two companies connected two industrial facilities in Bristol using 6km of fibre-optic cable that shared encryption keys using a stream of single photons.

Rather than only point-to-point, the new project will operate as a mesh, connecting various nodes to create end-to-end secure communications, according to Toshiba. But it faces several restrictions. Quantum cryptography protects the transport of the keys between the nodes; however, the nodes need to be placed in secure locations, which is usually the central office of the telecom operator.

"No cryptographic technology is trustless – you can't make cryptography technology without trusting someone," says Andrew Shields, head of the quantum technology division at Toshiba Europe. However, he adds, using multiple paths for keys in the network can protect against attack on any single node.

Another challenge is that the range of a single link within the network is 150-175km, which Toshiba hopes to extend. In June its Twin Field QKD system transported keys between nodes of 600km with the apparatus housed in a single lab.

Lewis says these are "not intractable" problems but simply need "engineering and technological development", which is under way.

In June, scientists at the University of Science and Technology of China created a secure quantum fibre link over 511km between two Chinese cities by using a relay in the middle that didn't have to be trusted.

Toshiba says its technology will eventually be used with satellites, for which it is working with Arqit, among others, for quantum fibre networks within national and continental areas, such as across Europe. The European Union has a similar ongoing project. The satellites will act as another trusted node creating a secure link between the various fibre networks in different regions.

This is no mean feat, points out Andersen Cheng, CEO of Post-Quantum, a company developing PQC technology. "JPMorgan has more than 5,000 branches; linking all of them using quantum fibre-optic cable may not be possible. It might just be key data centres are connected instead," he says.

Toshiba is targeting scale though. It recently announced it had developed the world's first chip-based QKD system that could in the future reduce the size and weight of the technology and enable mass manufacturing, making it applicable for IoT and other solutions.

"This will allow us to maybe even bring it into the home – we can think about a set-up like a set-top box. It will allow a much wider deployment of the technology in the future, it's difficult to tell when, but maybe in five to ten years' time," says Shields.

Ultimately just how worried should the world be about universal quantum computers being used to steal sensitive data or potentially starting cyber warfare? That depends on who you ask. Predictions range from the next few years to over ten. Williams says the incentive for a 'doomsday computer' that can steal everyone's information is practically unlimited, and therefore equal resources will be thrown at it.

Piers Clinton-Tarestad, a partner and global technology risk quantum computing leader at EY, says he advises clients to start thinking about the threat now, taking a risk-based approach. "If people wait for new standards to come out and then start looking at it, they're going to be behind the curve, but they shouldn't jump on the bandwagon either."

Professor Peter Kruger at Sussex University perhaps has the most reassuring answer: "I wouldn't be worried because the development of quantum cryptography is much faster than that of quantum computers," he says. "It's a race between the two and cryptography is currently winning."

12.Nuclear Quantum Computing: It's Coming

by Tristan Greene
https://thenextweb.com/news/nuclear-quantum-computing-its-coming

A trio of separate research teams from three different continents published individual papers indicating similar quantum computing breakthroughs yesterday. All three were funded in part by the US Army and each paper appears to be a slam dunk for the future of quantum computing.

But only one of them heralds the onset of the age of nuclear quantum computers.

It's about damn time

Maybe it's the whole concept of entanglement, but for a long time it's felt like we were suspended in a state where functional quantum machines were both "right around the corner" and "decades or more away."

But the past few years have seen a more rapid advancement toward functional quantum systems than most technologists could have imagined in their wildest dreams.

The likes of IBM, Microsoft, D-Wave, and Google putting hybrid quantum systems on the cloud coupled with the latter's amazing time crystal breakthrough have made 2018-2021 the opening years of what promises to be a golden age for quantum computing.

Despite this amazing progress, there are still holdouts who believe we'll never have a truly useful, fully-functional, qubit-based quantum computing system.

The main reason given by these cynics is usually because quantum systems are incredibly error-prone.

Not anymore?

The three new papers published yesterday (here, here, and here) should go a long way towards shutting those critics up because each of them manages to address the error-correction problem in quantum computing by, essentially, going back to the drawing board.

The first two teams, one from Tokyo and one from Los Angeles, went about the issue in a similar way while the Australian team decided to take a different approach.

In fact, it's worth noting that all three teams shared various resources in order to help facilitate each other's research.

The result is that each team was able to build a distinct, silicon-based, two-qubit quantum computing system capable of operating with greater than 99% accuracy.

So what?

That's pretty cool, but dozens of quantum research centers including IBM's, Google's, and Microsoft's have all developed functional quantum gate systems with dozens or even hundreds of qubits.

IBM and Google, for example, both claim they've reached "quantum advantage," or the point where their quantum computing systems can do things that no regular classical computing system could.

But here in 2022 we're not talking about being able to flip a switch and do quantum calculations. We're talking about cutting-edge computation systems that require enormous resources to pull off incredibly specific feats.

You can't just upload a neural network to a quantum computer and expect to act like it's been supercharged. The algorithms we're currently able to run on cutting-edge quantum systems are more like super-challenging math problems that can still be verified using classical means.

Unfortunately, the long and short of it is usually: the more qubits you have the more errors you get.

> The new research hopes to alleviate that by creating a new way to handle qubit operations, thus allowing gate-based quantum computer systems to scale.

And, right now, scalability is the single largest hurdle standing in the technology's way.

The solution?

It's actually fairly simple. All three teams are trying to put qubits on a silicon chip. As Ars Technica's John Timmer pointed out yesterday, this plays to our current engineering strengths:

> That possibility is what makes several results being published yesterday interesting. While there are differences among the three results being announced, they all have one thing in common: high-quality qubits produced in silicon. After all, if there's anything we know how to scale, it's silicon-based technologies.

What we found most interesting however, is the mind-boggling way in which the Australian team managed to create a pair of nearly errorless qubits: they went nuclear.

In a press release from the University of New South Wales, Mateusz Madzik, a lead author on the Australian team's research paper, described how entangling an electron with the nuclei of two phosphorous atoms allowed them to control them as qubits without losing information.

Per Madzik:

> If you have two nuclei that are connected to the same electron, you can make them do a quantum

operation.

While you don't operate the electron, those nuclei safely store their quantum information. But now you have the option of making them talk to each other via the electron, to realize universal quantum operations that can be adapted to any computational problem.

Is that safe?

Sure it is. They're not splitting atoms or fusing them, so there's probably a pretty close to zero chance that nothing bad will happen. We exploit atoms to do all kinds of things that don't involve blowing up entire cities.

In this case, the Australian team is exploiting a feature of entanglement that allows them to force communication between qubits that, normally, would either hoard their information or lose it too quickly for use.

It's likely just as safe as using lasers to create qubits out of light, maybe even safer. But the researchers are hoping it's the foundation for a paradigm that will be much easier to scale than other systems.

At the end of the day this is all exciting news. It's rare to see a peer-reviewed quantum computing breakthrough because the field is incredibly challenging. Getting three in the same day is a eureka moment in its own right.

Of course, it could take a while for these early experiments to pan out and turn into full-fledged quantum computers. But, if we take these papers as a proof-of-concept for the future, things look incredibly bright.

13.Groundbreaking Light Sources Can Increase Effectiveness And Security of Transferring Quantum Information

by Aalto University
https://phys.org/news/2022-01-groundbreaking-sources-effectiveness-quantum.html

Entanglement is a central phenomenon of quantum mechanics. It enables two photons to be connected with each other regardless of distance, and it is the basis of the immense potential of quantum technologies. However, the continuing development of quantum computers, cryptography, and sensors requires new, more efficient sources of entangled photon pairs.

Researchers at Aalto University plan to build a revolutionary LED light source to generate entangled photon pairs. The research group led by Professor Pertti Hakonen has received three-year funding from the Future Makers Funding Program of Technologies Finland Centennial Foundation and Jane and Aatos Erkko Foundation.

"Previously, entangled photons have been produced with non-linear crystals, which is extremely clumsy and rather inefficient, as just a few quantum pairs are extracted, and the generation process is random and has a low efficiency," Hakonen explains.

In the new project, the researchers will develop an effective, compact, bright and controllable source for entangled photons. Their approach is based on modern material science technologies which make it possible to create layers of single or few atoms, such as graphene, boron nitride, or molybdenum disulfide, and tailor them to form custom structures.

"The layer structure can be used to adjust whether the material is locally metallic or semiconducting and also whether it is a weak or strong semiconductor. The layered structure also enables electrons to tunnel—that is, to traverse the material—to produce entangled light," Hakonen says.

A step toward the quantum internet

Integrating an entangled photon generator into quantum processors would make fast quantum communication between separate processors possible even if they are far away from each other. Inter-connected individual quantum computers could form a quantum internet through which distributed quantum computing could be done.

"Due to distributed quantum computing large quantum processors can consist of simple superconducting quantum computers, avoiding significant practical issues in individual qubit operation," Hakonen explains.

Efficient entanglement generators are also in demand by the rapidly growing quantum cryptography field. Technologies for exchanging encryption keys via sharing entangled photons between the legitimate users promise to become the basis for unconditionally secure communications.

"Any attempt to eavesdrop would break the entanglement, which is easy to detect," Hakonen adds.

Professor Zhipei Sun and his group will participate in developing sample production techniques and the classification of entangled photons produced by the device. Hakonen and Sun have shared equipment for stacking ultrathin and reaction-sensitive layered structures. Ethan D. Minot, a professor at Oregon University and visiting professor at Aalto until summer 2022, also has a central role in the project. The cryotechnology partner of the project is Aalto's spinoff company Bluefors.

14.Quantum Computing is Coming. Now is The Right Time to Start Getting Ready

by Mark Samuels

https://www.zdnet.com/article/quantum-computing-is-coming-now-is-the-right-time-to-start-getting-ready/

From supporting a continuing shift to the cloud to embracing data-led services, CIOs already have a jam-packed digital transformation agenda for 2022 – and now the evidence suggests they need to make room for another line item: quantum computing.

"It will take some time – and therefore, now is the right moment to prepare for quantum," says Alberto Di Meglio, head of CERN openlab, who spoke at a recent event arranged by IBM Research.

CIOs who start investigating quantum will find a fast-growing area. Consultant Deloitte reports that venture capitalists invested more than $1bn into quantum-led businesses during 2021. The next 12 months will bring even more interest, with total VC spend likely to top $5bn by the end of the year.

This injection of cash will help technologists to develop reliable and useful quantum computers. That's a big priority right now, as efforts to boost the number of quantum bits – or qubits – available for computation will help businesses in their quests to identify potential use cases.

Deloitte recognises the nascent nature of quantum means practical applications remain thin on the ground. It estimates that fewer than a dozen companies worldwide will use quantum computers as part of their day-to-day operations this year.

But while quantum computing won't deliver big benefits during the next 12 months, Deloitte says the technology will generate billions of dollars in value annually one day, which is why CIOs should start preparing for quantum advantage now.

Evidence suggests that message is already getting through: three-quarters (74%) of senior executives believe organisations that fail to adopt quantum computing soon will fall behind quickly, according to a recent survey by quantum company Zapata Computing and Wakefield Research.

Di Meglio believes the secret to successfully understanding where your business might potentially create a quantum advantage is to focus on developments that are already being made around new instruments, tools, and methods of collaboration.

He says early preparatory work will help CIOs and their businesses to identify the right skills, technologies and partners for quantum success in the longer term.

As part of this process, CIOs and their executive partners must look to build collaborative teams, where all the necessary skills for quantum are brought together and then exploited in the most useful way.

"Quantum computing is a very multidisciplinary area. Organisations, institutions and universities really need to work to break the silos in-between these areas," he says.

Di Meglio says the most effective approach will be to create networks – or hubs – that allow people from across a wide ecosystem of internal and external partners to think about the challenges that businesses face and to posit potential quantum-based solutions.

"For us, the model of the hub is the right way of working," he says. "It is inherently about collaboration with all the other institutes and researchers across the world. Building this ecosystem is an essential ingredient to be able to move towards usable applications."

Panellists at the IBM Research event referred to pioneering approaches that are already underway, such as QUTACH in Germany, which brings together 10 major businesses to explore practical applications of quantum.

Deloitte suggests quantum chemistry, materials science and optimisation problems will likely be the first useful use cases to materialise. Transportation is another sector with quantum potential.

However, the path forward won't be as clear in all industries. If CIOs are going to convince their boards that it's worth spending time and money investigating the complex world of quantum computing, then the IT industry is going to have help tech chiefs build a strategy for collaboration and exploration.

Hannah Ventz, the head of the Competence Network for Quantum Computing at Fraunhofer Institute, Germany, says research organisations like her own must make it easy for companies to get their first experiences in quantum.

"We try to convince them that now is the right time," she says. "And then we offer experts to quantum labs and hubs where people can get their first experiences."

For CIOs who do want to give their staff exposure to quantum, Lidia del Rio, a physicist at ETH Zurich, says there's already a range of summer schools, hackathons and free online courses being run by some of the major tech firms.

However, del Rio also issues a word of warning. While these kinds of initiatives can help companies to build knowledge, there are still gaps in education programmes – particularly when it comes to the more technical elements of quantum.

"My one criticism about these things is that they focus on things that are already known, like algorithms, and they are restricted in range. I understand why – it's because these are the things that are easy to teach to a non-technical audience. But I think you need to have a much broader view of what quantum theory is," she says.

Del Rio says her organisation is aiming to raise awareness across industry and government about the risks and opportunities of all elements of quantum technology.

One of the key areas for consideration going forward will be governance. Arunima Sarkar, AI lead in the Centre for Fourth industrial Revolution at the World Economic Forum, says it's crucial that all interested parties – including CIOs – ensure any quantum advantage is exploited in an ethical way.

She says emerging technologies both shape society and are shaped by society. Businesses, technology firms and public bodies must work together now to ensure governing principles are established as use cases are discovered.

"I would say that the most appropriate and effective time to consider the societal, ethical and legal implications of technology is when the technology is still in the design and the development phase as it allows for early intervention," says Sarkar.

To this end, WEF has started a series of discussions with multi-stakeholder communities globally to debate ethical implications and potential risks of quantum. It has also initiated the creation of the first set of quantum computing governance principles.

"These are a set of shared principles that we believe will help guide the ecosystem for responsible development and innovation in this field," she says.

15.European Milestone: Quantum Computer With More Than 5,000 Qubits Launched

by Forschungszentrum Juelich
https://scitechdaily.com/european-milestone-quantum-computer-with-more-than-5000-qubits-launched/

A quantum annealer with more than 5,000 qubits has been put into operation at Forschungszentrum Jülich. The Jülich Supercomputing Centre (JSC) and D-Wave Systems, a leading provider of quantum computing systems, today launched the company's first cloud-based quantum service outside North America. The new system is located at Jülich and will work closely with the supercomputers at JSC in the future. The annealing quantum computer is part of the Jülich UNified Infrastructure for Quantum computing (JUNIQ), which was established in autumn 2019 to provide researchers in Germany and Europe with access to various quantum systems. Federal Minister of Education and Research Bettina Stark-Watzinger, Minister-President of North Rhine-Westphalia (NRW) Hendrik Wüst, and European Commissioner Mariya Gabriel officially put the system into operation during a ceremony held today, at which they highlighted the importance of collaboration in the development of practical quantum applications across industry sectors and research fields. The state government of NRW and the Federal Ministry of Education and Research (BMBF) are each providing € 5 million in funding to support the establishment of JUNIQ.

"Quantum computers promise enormous opportunities for our future and for research in Germany. They have the potential to transform our everyday lives for the better – with regard to making optimal use of our power grid, optimizing investment strategies in the financial market, or designing more effective medicines. This is why the Federal Research Ministry is providing intensive, broad-based support for quantum computer development. Today's launch of a quantum annealer in the JUNIQ user infrastructure is a further important step to propel Germany and Europe to an international leadership role in quantum computing."

— Federal Research Minister Bettina Stark-Watzinger

"Bringing quantum and supercomputing technologies together is key to supporting advanced scientific discoveries. It is like opening doors to new worlds with great innovation potential. Academics, businesses, and other organizations will be able to access this revolutionary technology now physically located in Europe, driving real-world value."

— Mariya Gabriel, European Commissioner

"The user infrastructure JUNIQ and the commissioning of the quantum annealer in Jülich impressively demonstrate North Rhine-Westphalia's development into a top European location for quantum computing. Our outstanding scientific landscape and the close networking of our players in science and industry make it possible to fully exploit the potential of these technologies."

— Minister-President of NRW Hendrik Wüst

Forschungszentrum Jülich has set itself the goal of establishing a leading development and user community from industry and science for quantum computing applications in Germany and throughout Europe. "To achieve this goal, we established JUNIQ as a user facility for open innovations at the Jülich Supercomputing Centre in 2019. It provides users with a uniform quantum computing platform as a service and also offers them the relevant expertise for user support and joint software development," explains Prof. Wolfgang Marquardt, Chairman of the Board of Directors of Forschungszentrum Jülich. "Through JUNIQ, we provide users and developers with service-oriented access to our unique Jülich quantum computing ecosystem. This offers users the best conditions to rapidly accelerate the utilization of quantum computers thanks to its excellent technical infrastructure and, above all, the pooling of our considerable expertise in the fields of supercomputing and quantum technologies."

The new quantum system is the second D-Wave quantum computer to be used within the JUNIQ user infrastructure and is the world's first Advantage quantum annealer to be located outside the company's home country, Canada. "We operate the system directly here at Jülich. This gives us the opportunity to integrate it closely with our supercomputing infrastructure," explains Prof. Kristel Michielsen, a quantum computing pioneer and head of the Quantum Information Processing group at JSC. This enables experts at Jülich to gain experience in operating and maintaining such a machine and helps to transfer important knowledge to Germany. Moreover, access to this system is subject to German legislation and checks.

"Given the extent to which companies and research institutions are identifying important problems that require investments in quantum computing, the marketing potential for quantum computing will grow at a faster rate than ever before," says Alan Baratz, CEO at D-Wave Systems. "This particularly applies to Europe, where we are seeing increasing interest from companies, universities, and even government institutions. We look forward to combining Jülich's expertise in the field of deep computing with D-Wave's ability to scale and commercialize transformative technologies. I am proud that this is the first commercial quantum computimg system in-region in Europe, deepening the impact of quantum computing in Europe and am excited about the innovations and applications that will emerge from the system."

The new system is an annealing quantum computer. This type of quantum system is particularly well suited for solving challenging optimization problems that are particularly relevant to industry. These include the efficient control of traffic flows and the training of neural networks for artificial intelligence applications. D-Wave is a leading manufacturer of such quantum systems. Clients of the company have developed early quantum applications in a diverse range of areas such as financial modeling, flight planning, election modeling, quantum chemistry simulation, automotive engineering, healthcare, logistics, and more.

"We're also looking at ways to integrate the new system into our supercomputing infrastructure. At that time, to the best of our knowledge, this would be the first instance of a quantum computer working directly with a supercomputer," says Prof. Thomas Lippert, director of the Jülich Supercomputing Centre. "This is made possible because the quantum annealer has over 5,000 qubits and is therefore big enough to help with application-related problems that are typically calculated on supercomputers." The quantum annealer is a quantum computer that has been developed with a view to industrial applications. It also has a number of special features that users of the JUNIQ infrastructure can access, such as the new Advantage performance update, incorporating the highly connected Pegasus topology, and unprecedented high performance in a commercial quantum system.

16.Towards Compact Quantum Computers, Thanks to Topology

by JuLien Levallois
https://www.swissquantumhub.com/towards-compact-quantum-computers-thanks-to-topology/

By now, the future of computing is inconceivable without quantum computers. For the most part, these are still in the research phase. They hold the promise of speeding up certain calculations and simulations by orders of magnitude compared to classical computers.

Quantum bits, or qubits for short, form the basis of quantum computers. So-called topological quantum bits are a novel type that might prove to be superior. To find out how these could be created, an international team of researchers has carried out measurements at the Swiss Light Source SLS at PSI.

More stable quantum bits

"Computer bits that follow the laws of quantum mechanics can be achieved in different ways," explains Niels Schröter, one of the study's authors. He was a researcher at PSI until April 2021, when he moved to the Max Planck Institute of Microstructure Physics in Halle, Germany. "Most types of qubits unfortunately lose their information quickly; you could say they are forgetful qubits." There is a technical solution to this: Each qubit is backed up with a system of additional qubits that correct any errors that occur. But this means that the total number of qubits needed for an operational quantum computer quickly rises into the millions.

"Microsoft's approach, which we are now collaborating on, is quite different," Schröter continues. "We want to help create a new kind of qubit that is immune to leakage of information. This would allow us to use just a few qubits to achieve a slim, functioning quantum computer."

The researchers hope to obtain such immunity with so-called topological quantum bits. These would be something completely new that no research group has yet been able to create.

Topological materials became more widely known through the Nobel Prize in Physics in 2016. Topology is originally a field of mathematics that explores, among other things, how geometric objects behave when they are deformed. However, the mathematical language developed for this can also be applied to other physical properties of materials. Quantum bits in topological materials would then be topological qubits.

Quasiparticles in semiconductor nanowires

It is known that thin-film systems of certain semiconductors and superconductors could lead to exotic electron states that would act as such topological qubits. Specifically, ultra-thin, short wires made of a semiconductor material could be considered for this purpose. These have a diameter of only 100 nanometres and are 1,000 nanometres (i.e., 0.0001 centimetres) long. On their outer surface, in the longitudinal direction, the top half of the wires is coated with a thin layer of a superconductor. The rest of the wire is not coated so that a natural oxide layer forms there. Computer simulations for optimising these components predict that the crucial, quantum mechanical electron states are only located at the interface between the semiconductor and the superconductor and not between the semiconductor and its oxide layer.

"The collective, asymmetric distribution of electrons generated in these nanowires can be physically described as so-called quasiparticles," says Gabriel Aeppli, head of the Photon Science Division at PSI, who was also involved in the current study. "Now, if suitable semiconductor and superconductor materials are chosen, these electrons should give rise to special quasiparticles called Majorana fermions at the ends of the nanowires."

Majorana fermions are topological states. They could therefore act as information carriers, ergo as quantum bits in a quantum computer. "Over the course of the last decade, recipes to create Majorana fermions have already been studied and refined by research groups around the world," Aeppli continues. "But to continue with this analogy: we still didn't know which cooking pot would give us the best results for this recipe."

Indium antimonide has the advantage

A central concern of the current research project was therefore the comparison of two "cooking pots". The researchers investigated two different semiconductors and their natural oxide layer: on the one hand indium arsenide and on the other indium antimonide.

At SLS, the PSI researchers used an investigation method called soft X-ray angle-resolved photoelectron spectroscopy – SX-ARPES for short. A novel computer model developed by Noa Marom's group at Carnegie Mellon University, USA, together with Vladimir Strocov from PSI, was used to interpret the complex experimental data. "The computer models used up to now led to an unmanageably large number of spurious results. With our new method, we can now look at all the results, automatically filter out the physically relevant ones, and properly interpret the experimental outcome," explains Strocov.

Through their combination of SX-ARPES experiments and computer models, the researchers have now been able to show that indium antimonide has a particularly low electron density below its oxide layer. This would be advantageous for the formation of topological Majorana fermions in the planned nanowires.

"From the point of view of electron distribution under the oxide layer, indium antimonide is therefore better suited than indium arsenide to serve as a carrier material for topological quantum bits," concludes Niels Schröter. However, he points out that in the search for the best materials for a topological quantum computer, other advantages and disadvantages must certainly be weighed against each other. "Our advanced spectroscopic methods will certainly be instrumental in the quest for the quantum computing materials," says Strocov. "PSI is currently taking big steps to expand quantum research and engineering in Switzerland, and SLS is an essential part of that."

17.Donot Hacking Team Targeting Government And Military Entities in South Asia

by Ravie Lakshmanan
https://thehackernews.com/2022/01/donot-hacking-team-targeting-government.html

A threat actor with potential links to an Indian cybersecurity company has been nothing if remarkably persistent in its attacks against military organizations based in South Asia, including Bangladesh, Nepal, and Sri Lanka, since at least September 2020 by deploying different variants of its bespoke malware framework.

Slovak cybersecurity firm ESET attributed the highly targeted attack to a hacking group known as Donot Team. "Donot Team has been consistently targeting the same entities with waves of spearphishing emails with malicious attachments every two to four months," researchers Facundo Muñoz and Matías Porolli said.

Operating since at least 2016, Donot Team (also known as APT-C-35 and SectorE02) has been linked to a string of intrusions primarily targeting embassies, governments, and military entities in Bangladesh, Sri Lanka, Pakistan, and Nepal with Windows and Android malware.

In October 2021, Amnesty International unearthed evidence tying the group's attack infrastructure to an Indian cybersecurity company called Innefu Labs, raising suspicions that the threat actor may be selling the spyware or offering a hackers-for-hire service to governments of the region.

While it's not uncommon for APT groups to re-attack a previously compromised network by deploying stealthier backdoors to cover up their tracks, Donot Team tries a different tack in that it deploys multiple variants of the malware already in its arsenal.

Delivered via weaponized Microsoft Office documents, the so-called yty malware framework is a chain of intermediary downloaders that culminates in the execution of a backdoor, which takes care of retrieving additional components capable of harvesting files, recording keystrokes and screenshots, and deploying reverse shells for remote access.

ESET dubbed the new variants of yty, DarkMusical and Gedit, with telemetry data pointing to attacks from a third variant called Jaca from March to July 2021. The first wave of attacks using DarkMusical is said to have occurred in June 2021, while Gedit-related campaigns were observed as early as September 2020, only to pick up the pace a year later.

What's more, a fourth set of attacks that happened between February and March 2021 targeting military organizations in Bangladesh and Sri Lanka leveraged a modified version of Gedit codenamed Henos.

"Donot Team makes up for its low sophistication with tenacity," the researchers concluded. "We expect that it will continue to push on regardless of its many setbacks. Only time will tell if the group evolves its current TTPs and malware."

18.Inner Workings of Quantum Computers

by Doe/Sandia National Laboratories
https://www.sciencedaily.com/releases/2022/01/220119121450.htm

Two papers published today in the scientific journal Nature describe how separate research teams -- one including Sandia researchers -- used a Sandia technique called gate set tomography to develop and validate highly reliable quantum processors. Sandia has been developing gate set tomography since 2012, with funding from the DOE Office of Science through the Advanced Scientific Computing Research program.

Sandia scientists collaborated with Australian researchers at the University of New South Wales in Sydney, led by Professor Andrea Morello, to publish one of today's papers. Together, they used GST to show that a sophisticated, three-qubit system comprising two atomic nuclei and one electron in a silicon chip could be manipulated reliably with 99%-plus accuracy.

In another Nature article appearing today, a group led by Professor Lieven Vandersypen at Delft University of Technology in the Netherlands used gate set tomography, implemented using Sandia software, to demonstrate the important milestone of 99%-plus accuracy but with a different approach, controlling electrons trapped within quantum dots instead of isolated atomic nuclei.

"We want researchers everywhere to know they have access to a powerful, cutting-edge tool that will help them make their breakthroughs," said Sandia scientist Robin Blume-Kohout.

Future quantum processors with many more qubits, or quantum bits, could enable users working in national security, science and industry to perform some tasks faster than they ever could with a conventional computer. But flaws in current system controls cause computational errors. A quantum computer can correct some errors, but the more errors it must correct, the larger and more expensive that computer becomes to build.

So, scientists need diagnostic tools to calculate how precisely they can control single atoms and electrons that store qubits and learn how to prevent errors instead of correcting them. This increases the reliability of their system while keeping costs down.

Gate set tomography is Sandia's flagship technique for measuring the performance of qubits and quantum logic operations, also known as "gates." It combines results from many kinds of measurements to generate a detailed report describing every error occurring in the qubits. Experimental scientists like Morello can use the diagnostic results to deduce what they need to fix.

"The Quantum Performance Laboratory at Sandia National Labs, led by Robin Blume-Kohout, has developed the most accurate method to identify the nature of the errors occurring in a quantum computer," Morello said.

Gate set tomography even detects unexpected error

The Sandia team maintains a free, open-source GST software called pyGSTi (pronounced "pigsty," which stands for Python Gate Set Tomography Implementation). Publicly available at http://www.pygsti.info, it was used by both research groups publishing in Nature today.

While the Delft team used the pyGSTi software without assistance from the Sandia team, the UNSW-Sandia collaboration used a new, customized form of gate set tomography developed by the Sandia researchers. The new techniques enabled the team to rule out more potential error modes and focus on a few dominant error mechanisms.

But when the Sandia team studied the GST analysis of the UNSW experimental data, they discovered a surprising kind of error that Morello's group did not expect. The nuclear-spin qubits were interacting when they should have been isolated. Concerned that this error might indicate a flaw in the qubits, the team turned to Sandia's Andrew Baczewski, an expert in silicon qubit physics and a researcher at the Quantum Systems Accelerator, a National Quantum Information Science Research Center, to help find its source.

"It came to occupy a lot of my free time," Baczewski said. "I would be out for a walk on a Saturday morning and, out of the blue, something would occur to me and I would run home and do math for an hour."

Eventually, Baczewski and the rest of the team tracked the error to a signal generator that was leaking microwaves into the system. This can be easily fixed in future experiments, now that the cause is known.

Blume-Kohout said, "It was really fulfilling to see confirmation that GST even detected the errors that nobody expected."

"The collaboration with Sandia National Laboratories has been crucial to achieve the milestone of high-fidelity quantum operations in silicon," Morello said. "The theoretical and computational methods developed at Sandia have enabled the rigorous demonstration of quantum computing with better than 99% fidelity and have provided precious insights into the microscopic causes of the residual errors. We plan to expand this strategic collaboration in years to come."

19.How France Is Becoming A Quantum Computing Power

by Peter Suciu
https://nationalinterest.org/blog/buzz/how-france-becoming-quantum-computing-power-199691

A year ago French president Emmanuel Macron announced plans to provide a framework for his nation's industrial and research forces to make the country a key player in the development of quantum technology. The "Quantum Plan" included an investment of €1.8 billion ($2 billion) over five years—a significant increase that placed France third after the United States and China.

That included nearly €800 million for computers alone.

The sector has already experienced significant growth, with patent filings doubling between 2018 and 2020, according to data and analytics company GlobalData. It is believed that the technology could potentially revolutionize areas of defense such as artificial intelligence (AI), enabling autonomous vehicles and improved targeting for precision weapons systems.

Quantum Leap Forward

Quantum computers are not just improved computers. Rather the machines—once fully developed—could utilize the properties of quantum physics to store data and perform computations. Theoretically, a single quantum computer could complete in seconds tasks that would take classical computers thousands or even millions of years.

The first nation to achieve quantum computing could have a significant advantage, especially as the technology could render current encryption obsolete.

According to a new report from GlobalData, "Quantum Technologies in Defense," this is why many countries are concerned about falling behind in the quantum race due to the potential for the technology to revolutionize communications. Communication is a critical area for the defense sector, with quantum key distribution (QKD) having the potential to completely prevent adversaries from accessing secure communications.

Per the report: "As the existing quantum workforce is extremely small, with only a limited number of people having the capability to design and build quantum computers, countries are pushing to develop an industrial and skills base that will enable them to utilize quantum technologies."

Part of France's spending will initially be to create a platform that will allow traditional computers to access quantum processing power. "Quantum computers are expensive and extremely complex to build, so a remote platform is critical for providing the defense industry with access to quantum tools," explained William Davies, associate defense analyst at GlobalData, in an email.

"The technology is an important investment for the future of the French defense industry, and is a good move for the country to keep up with its peers," Davies continued. "Allies such as the U.S. and the UK are also investing, as well as adversaries such as China, largely to benefit their own defense interests. Further, IQM, a European quantum computer company, is opening an office in Paris in 2022 as a direct response to France increasing investment in quantum. This business investment will provide opportunities for France to expand its domestic quantum base and increase the amount of trained personnel in the sector."

Along with hypersonic weapons, stealth technology, and high-energy weapons, quantum computing could be a significant game changer. Clearly France intends not to be left behind.

20.Israeli Quantum Cryptographic Solutions Provider QuantLR Integrates With Nvidia

by Noga Martin
https://www.israelhayom.com/2022/01/19/israeli-quantum-cryptographic-solutions-provider-quantlr-integrates-with-nvidia/

Quantum Key Distribution (QKD) company QuantLR Ltd, based in Modi'in, has integrated its technology with NVIDIA's suite of networking offerings, paving the way towards a quantum-secured data center, the company announced Tuesday.

QuantLR aims to provide versatile, low-cost quantum cryptographic solutions based on QKD technologies to protect communicated data.

As part of the project, QuantLR's QKD system connected and transferred encryption keys to two NVIDIA ConnectX-6 NICs. The interface was achieved using the ETSI REST-based key delivery API. During the process, different scenarios were tested: using different fiber lengths, attenuations and key distribution rates.

The QuantLR-NVIDIA project was executed as part of a consortium that partially funded by the Israel Innovation Authority (IIA) and the Defense Ministry's Directorate of Defense Research & Development, with support from the Israeli Quantum initiative led by Dr. Tal David.

"We are happy to be supported by NVIDIA in advancing Quantum encryption solutions that are proven to be the only completely secured solutions against any eavesdropping and hacking attempts to communication lines in the present, and in the future," said QuantLR CEO Shlomi Cohen.

"The support of a leading company such as NVIDIA accelerates our development process and enables us to offer the market an affordable solution sooner. The quantum encryption market is predicted to reach sales volumes of more than $7B in 2025, and we plan to be a significant player in this market," Cohen said.

Kevin Deierling, Senior Vice President of Networking at NVIDIA, said, "The growth of game-changing innovations such as AI, 5G and smart devices continues to grow the volume of traffic and sensitive information in today's data centers. NVIDIA's collaboration with QuantLR enables next-generation cybersecurity technologies that stay ahead of emerging threats to the data center."

21.Major Breakthrough As Quantum Computing in Silicon Hits 99% Accuracy

by University of New South Wales
https://scitechdaily.com/major-breakthrough-as-quantum-computing-in-silicon-hits-99-accuracy/

Australian researchers have proven that near error-free quantum computing is possible, paving the way to build silicon-based quantum devices compatible with current semiconductor manufacturing technology.

"Today's publication in Nature shows our operations were 99% error-free," says Professor Andrea Morello of UNSW, who led the work.

"When the errors are so rare, it becomes possible to detect them and correct them when they occur. This shows that it is possible to build quantum computers that have enough scale, and enough power, to handle meaningful computation."

This piece of research is an important milestone on the journey that will get us there," Prof. Morello says.

Quantum computing in silicon hits the 99% threshold

Morello's paper is one of three published today in Nature that independently confirm that robust, reliable quantum computing in silicon is now a reality. This breakthrough features on the front cover of the journal.

- Morello et al achieved 1-qubit operation fidelities up to 99.95%, and 2-qubit fidelity of 99.37% with a three-qubit system comprising an electron and two phosphorous atoms, introduced in silicon via ion implantation.

- A Delft team in the Netherlands led by Lieven Vandersypen achieved 99.87% 1-qubit and 99.65% 2-qubit fidelities using electron spins in quantum dots formed in a stack of silicon and silicon-germanium alloy (Si/SiGe).

- A RIKEN team in Japan led by Seigo Tarucha similarly achieved 99.84% 1-qubit and 99.51% 2-qubit fidelities in a two-electron system using Si/SiGe quantum dots.

The UNSW and Delft teams certified the performance of their quantum processors using a sophisticated method called gate set tomography, developed at Sandia National Laboratories in the U.S. and made openly available to the research community.

Morello had previously demonstrated that he could preserve quantum information in silicon for 35 seconds, due to the extreme isolation of nuclear spins from their environment. "In the quantum world, 35 seconds is an eternity," says Prof. Morello. "To give a comparison, in the famous Google and IBM superconducting quantum computers the lifetime is about a hundred microseconds – nearly a million times shorter."

But the trade-off was that isolating the qubits made it seemingly impossible for them to interact with each other, as necessary to perform actual computations.

Nuclear spins learn to interact accurately

Today's paper describes how his team overcame this problem by using an electron encompassing two nuclei of phosphorus atoms.

"If you have two nuclei that are connected to the same electron, you can make them do a quantum operation," says Dr. Mateusz Madzik, one of the lead experimental authors.

"While you don't operate the electron, those nuclei safely store their quantum information. But now you have the option of making them talk to each other via the electron, to realize universal quantum operations that can be adapted to any computational problem."

"This really is an unlocking technology," says Dr. Serwan Asaad, another lead experimental author. "The nuclear spins are the core quantum processor. If you entangle them with the electron, then the electron can then be moved to another place and entangled with other qubit nuclei further afield, opening the way to making large arrays of qubits capable of robust and useful computations."

David Jamieson, research leader at the University of Melbourne, adds: "The phosphorous atoms were introduced in the silicon chip using ion implantation, the same method used in all existing silicon computer chips. This ensures that our quantum breakthrough is compatible with the broader semiconductor industry."

All existing computers deploy some form of error correction and data redundancy, but the laws of quantum physics pose severe restrictions on how the correction takes place in quantum computer. Prof. Morello explains: "You typically need error rates below 1 percent, to apply quantum error correction protocols. Having now achieved this goal, we can start designing silicon quantum processors that scale up and operate reliably for useful calculations."

22.Innovative New Algorithms Advance The Computing Power of Early-Stage Quantum Computers

by Ames Laboratory
https://scitechdaily.com/innovative-new-algorithms-advance-the-computing-power-of-early-stage-quantum-computers/

A group of scientists at the U.S. Department of Energy's Ames Laboratory has developed computational quantum algorithms that are capable of efficient and highly accurate simulations of static and dynamic properties of quantum systems. The algorithms are valuable tools to gain greater insight into the physics and chemistry of complex materials, and they are specifically designed to work on existing and near-future quantum computers.

Scientist Yong-Xin Yao and his research partners at Ames Lab use the power of advanced computers to speed discovery in condensed matter physics, modelling incredibly complex quantum mechanics and how they change over ultra-fast timescales. Current high performance computers can model the properties of very simple, small quantum systems, but larger or more complex systems rapidly expand the number of calculations a computer must perform to arrive at an accurate model, slowing the pace not only of computation, but also discovery.

"This is a real challenge given the current early-stage of existing quantum computing capabilities," said Yao, "but it is also a very promising opportunity, since these calculations overwhelm classical computer systems, or take far too long to provide timely answers."

The new algorithms tap into the capabilities of existing quantum computer capabilities by adaptively generating and then tailoring the number and variety of "educated guesses" the computer needs to make in order to accurately describe the lowest-energy state and evolving quantum mechanics of a system. The algorithms are scalable, making them able to model even larger systems accurately with existing current "noisy" (fragile and prone to error) quantum computers, and their near-future iterations.

"Accurately modelling spin and molecular systems is only the first part of the goal," said Yao, "In application, we see this being used to solve complex materials science problems. With the capabilities of these two algorithms, we can guide experimentalists in their efforts to control materials' properties like magnetism, superconductivity, chemical reactions, and photo-energy conversion."

"Our long-term goal is to reach 'quantum advantage' for materials — to utilize quantum computing to achieve capabilities that cannot be achieved on any supercomputer today," said Ames Laboratory Scientist Peter Orth.

This topic is further discussed in two papers: (1)"Adaptive Variational Quantum Dynamics Simulation," authored by Y.-X. Yao, N. Gomes, F. Zhang, C.-Z. Wang, K.-M. Ho, T. Iadecola, and P. P. Orth; and published in PRX Quantum; (2) "Adaptive Variational Quantum Imaginary Time Evolution Approach for Ground State Preparation," authored by N. Gomes, A. Mukherjee, F. Zhang, T. Iadecola, C.-Z. Wang, K.-M. Ho, P. P. Orth, Y.-X. Yao; accepted in Advanced Quantum Technologies.

Ames Laboratory is a U.S. Department of Energy Office of Science National Laboratory operated by Iowa State University. Ames Laboratory creates innovative materials, technologies and energy solutions. We use our expertise, unique capabilities and interdisciplinary collaborations to solve global problems.

Ames Laboratory is supported by the Office of Science of the U.S. Department of Energy. The Office of Science is the single largest supporter of basic research in the physical sciences in the United States, and is working to address some of the most pressing challenges of our time.

23.Securing IoT With Quantum Cryptography

by Roland Atoui
https://www.iotforall.com/securing-iot-with-quantum-cryptography

The Internet of Things (IoT) is a growing technology that continues to gain traction year after year. On the one hand, it can be helpful, but on the other hand, it carries many security threats. These threats include scalable remote attacks, side-channel attacks on cryptography, DDoS attacks, data breaches, malware, and others.

Why Use Quantum Cryptography?

Classical cryptographic algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm, can work well with classical computers. But the technology is beginning to shift towards quantum computing, and quantum computing has excellent processing power. It can easily break the current cryptographic algorithms. That is why we need to design quantum cryptographic algorithms: to prevent security breaches before quantum computers come into commercial use.

Why Secure IoT?

IoT devices could have many security loopholes covering the hardware and software, the network, or users. Hacking techniques have advanced so much over the past few years. Attackers use more state-of-the-art means, which represents a significant threat to IoT security. This is why not quantum is used at some point. The security protection measures implemented by design have to ensure that IoT devices cannot be easily hacked today. Furthermore, devices should be protected ten years from now. Long lifespans of IoT devices mean that they need future-proof defenses.

How Does Quantum Cryptography Work?

Of course, technical quantum solutions are challenging to implement in IoT devices due to technical and commercial constraints. Therefore, a few security options combine both the quantum and classical approaches.

One option keeps the current semiconductor chips but uses quantum techniques to create a unique long cryptographic key for every device. This can be done with a quantum random number generation (QRNG). It creates a noise source with a high randomness level.

Quantum computing can generate large numbers at lightning speed. Hence, the communications can be safe, and the key can be secured. This means every device will have a unique key and each key will be tough to crack. The only way to get the key would be to access the physical device configuration. But doing that without getting noticed in tamper-resistant devices would be very difficult.

Conclusion

Although quantum cryptography and quantum computing have developed quite efficiently, some more advancement is necessary for them to become a reality in commercial systems. Commercial use is a big challenge. Firstly, implementing quantum systems in IoT is expensive. Secondly, large-scale quantum apparatus is hard to afford for many organizations. Thirdly, the properties of photons restrict them from traveling long distances. If these issues can be resolved, we will have successful IoT systems with quantum cryptography. That will make them the most secure modern systems.

Finally, we strongly recommend you start from the basics to secure your IoT devices and systems by monitoring state-of-the-art of quantum cryptography before deciding to buy or use a secure component in your IoT product.

24.Finland Moves to Industrialise Quantum Computing

by Pat Brans
https://www.computerweekly.com/feature/Finland-moves-to-industrialise-quantum-computing

The Finnish Ministry of Economic Affairs recently funded an innovation project for VTT Technical Research Centre of Finland to build the country's first quantum computer.

VTT enlisted IQM, a homegrown startup, to help with the project, which began at the end of 2020 and will continue until 2024.

Owned by the Finnish state, VTT is one of Europe's leading research institutions. It plays the crucial role of taking what researchers learn in a range of scientific domains and making it ready for industry. The government firmly believes the best way to ready quantum computing for industry is to build a working quantum computer.

“When it comes to quantum technology, Finland has one of those unique opportunities where a small country has a whole value chain in place,” says Himadri Majumdar, programme manager for the Quantum Initiative at VTT. “Other countries also have strong ecosystems in quantum technologies, but in almost all cases they are working on a lot of different topics and many different platforms. Finnish researchers focus almost exclusively on the superconducting qubit approach, which they have been using for years and know very well.”
This will not be the first time Finland took quantum technology from research to industrialisation. They already did so for quantum sensors. Finnish spin-off companies have been producing sensors based on quantum technology since the 1980s and the 1990s, in the form of superconducting quantum interference devices (Squids), which were commercialised as essential components in brain imaging systems. Finnish startups also commercialised terahertz spectroscopy and terahertz imaging – quantum technologies used in space applications and in scanners at airports.

The country is now well positioned to play a significant role in the next generation of quantum devices and sensors – for example, atomic clocks scaled down to small dimensions and used in consumer devices. Given the success Finland has had with other quantum technologies, the government is hoping to get ahead of the curve on quantum computers.

“Now is the right time for us to lay the groundwork for bringing quantum computing to industry,” says Majumdar. “At the end of last year, we built a five-qubit computer. The ultimate measure of success is to run a programme on it and benchmark the results. We are developing the software stacks we will need to do this in early 2022.”

We don’t expect to solve any practical problems with five qubits. But the device can serve as an excellent proof of concept. The project team will then expand the computing capacity with 20 qubits in 2022 – and then with 50 qubits by the end of 2024, when they hope to solve real problems.

“We think the 2020s is a crucial decade for building the fundamentals,” says Majumdar. “This is when the race for making a higher number of qubits is happening. There will be two parallel paths. The first one is the one we have already started: building a computer with a large number of NISQ [noisy intermediate-scale quantum] qubits. The second path, which will also be taken during this decade, is to find ways of building pure qubits – that is, qubits that are not noisy and do not need error correction.”

Growing ecosystems in Finland

To assist in the project of building a quantum computer, VTT chose IQM, a Finnish startup that was founded in 2019 and now has 140 employees. “We act as a systems integrator,” says Jan Goetz, CEO and co-founder of IQM. “Our job is to take the different pieces and build quantum computing systems.”

One of the pieces they use is the cryogenic system from Finnish company Bluefors, which grew out of Finland’s long history of research in cold temperature physics. Founded in 2008, Bluefors eventually found a niche in quantum computing and is now the world's leading provider of the cryogenic enclosures used to keep superconducting qubits at temperatures very close to absolute zero.

"Since we built Finland's first quantum computer this year, we have seen a few other startups emerge," says Goetz. "Algorithmiq is one of them, and Quanscient is another one that just very recently formed. On top of that, several companies from outside of Finland have seen an opportunity here and are now part of the local ecosystem. With this combination of homegrown startups and the local subsidiaries of foreign firms, we now have a nice ecosystem of organisations forming around quantum computing."

While virtually all industrialised nations in the world recognise quantum computing as a strategic technology, Finland is particularly well positioned to embrace the new paradigm. The government is hoping to increase the advantage through investment – and some of the local companies and research organisations are also benefiting from EU initiatives, as well as the venture capital that is now flowing into Finland to cash in on the country's skill set.

Research and educational ecosystems are also sprouting up, with plans to hire more scientists and professors. VTT, Aalto University and Helsinki University are founding members of a research community called InstituteQ, which focuses on developing world-class quantum expertise and helping business make use of quantum computing.

The Finns are acutely aware that Finland can never be a Silicon Valley. The economy just isn't big enough. Finnish startups therefore know from the beginning that they must ready their products and services for export – and this is what makes homegrown Finnish companies so strong on the world market.

"As for IQM, we want to be the main supplier for supercomputing centres and for companies that can afford their own quantum computers," says Goetz. "As systems integrator, we deliver a full system. But the system, of course, will contain more than just IQM parts.

"We built the heart ourselves, which is the quantum processor, and then a little bit of the control electronics and part of the software. The software is best described as a firmware stack, but all the rest we just assemble," he says. "We buy the cryogenics from Bluefors, we buy cables, and we buy amplifiers. Then we bring it all together."

IQM manufactured the qubits for the five-qubit prototype and will continue up to the 50-qubit computer, which is expected to be a working system that can solve real problems. IQM has its own fabrication line, which it uses to build the processor, starting with bare silicon wafers. They also use the Otanano national infrastructure, which features the largest R&D cleanroom in the Nordic countries and is jointly run by VTT and Aalto University.

A new usage model will one day arise

One good way of illustrating how quantum computers might be used is to consider how Google Maps finds the best path. This is a very compute-intensive problem. If you request this on your smartphone, it's not your smartphone that calculates the path. Your smartphone only communicates the problem to a server somewhere in a datacentre. The path is calculated on some powerful computer and the answer is transmitted back to your phone.

Quantum computing services will probably be offered to consumers in this way in the future, with most users completely unaware of what is involved. Quantum computing will also help companies with R&D using a similar model. Companies that want to find new materials can request modelling and simulation services, and some parts of those services will be performed by a quantum computer in the cloud; others will be performed by a classical computer.

IBM and other companies already offer quantum computing services on the cloud. But those services are used by researchers and are often limited to simulating quantum computing. Researchers can test algorithms on the simulators – and those who have a few qubits themselves can compare the results of the simulator with what they get on their prototype quantum computer.

It's not yet clear how a practical system will offer services to application developers and end users. One approach is to have specific libraries – for example, a chemistry library that can be used to simulate new molecules. Application developers need only access these libraries to develop a solution that will help companies with R&D. At run time, the library transfers the work to a supercomputing centre that does the work. When the supercomputing centre gets a task, it separates the parts that go to the quantum computer from those that can be better performed on a classical computer. To do this, it will need a scheduler.

"Something very similar is already occurring for AI algorithms," says Goetz. "People use GPU [graphical processing units] to accelerate CPU clusters. Certain problems run very well on GPUs, but not well at all on CPUs. These problems are separated and assigned to the appropriate processing units.

"To have the libraries, of course, you need to have the algorithms and the compilers in-between, and that's a tricky topic right now," he says. "We're not yet at the point where we have a large-scale universal quantum computer where you just have one type of compiler that compiles everything for a standard architecture."

Device architecture

Quantum computers are far from generic. Writing a program requires knowledge of the architecture of a given device – including the quality of the qubits and the distances between them. Coherence and fidelity are the most important factors to consider.

"Let's say on the processor you have a few bad qubits," says Goetz. "You want to avoid them in your calculation and let them only do very minor tasks. In the future, maybe we will have a system of feedback between the processor and the actual compiler, so the compiler can generate programs that fit the computer. But for now, we're still in this phase where people really need to get their hands dirty and map the two worlds together.

"To help developers, we are building a kind of firmware that will provide standard software interfaces," he says. "Right now, we're integrating into Google Cirq, IBM Qiskit and Atos QLM [Quantum Learning Machine]. These are the three main software layers on top. Anybody with software that runs on top of those layers will be able to run on our machines."

The first practical applications of quantum computing

As part of the project funded by the Finnish Ministry of Economic Affairs, a separate team in VTT, the quantum algorithm team, is developing algorithms to be used on the quantum computer. Materials modelling is one example of an application area they are working on. VTT intends to take a few such examples to test the algorithms on the five-qubit systems and compare the results with a simulation.

Like many other organisations trying to build a practical quantum computer, VTT is looking at two broad types of applications. The first is to solve complex optimisation problems that exist in many industries – problem domains, such as energy distribution, process control and fleet management. The second is to predict the structures and properties of molecular formations much more accurately and effectively than before, accelerating drug discovery and the development of new materials.

"Nobody knows whether the first practical applications of quantum computing will be in finance, in medicine, materials science or some other area," says Majumdar. "But one thing that's for sure is that it will evolve very quickly.

"A trend we are already starting to see is buyers and end users of the technology (BMW, Goldman Sachs and others) tend to create a triangle of companies, consisting of a hardware company, a software company and themselves as users. This triangle develops a highly customised solution around a specific use case. This trend will continue for quite a few years because quantum computers are very specific and machine agnostic algorithms are a long way off. Everything will be highly tailored in the beginning."

While there are still a lot of unknowns, one thing is clear: by building a local ecosystem that exports products and expertise, Finland stands a good chance of becoming a part of the European answer to the quantum computing technology coming out of the US and China.

25.Log4J: Google And IBM Call For List of Critical Open Source Projects

by Jonathan Greig
https://www.zdnet.com/article/log4j-after-white-house-meeting-google-calls-for-list-of-critical-open-source-projects/

Google and IBM are urging tech organizations to join forces to identify critical open source projects after attending a White House meeting on open source security concerns.

The meeting, led by White House cybersecurity leader Anne Neuberger, included officials from organizations like Apache, Google, Apple, Amazon, IBM, Microsoft, Meta, Linux, and Oracle as well as government agencies like the Department of Defense and the Cybersecurity and Infrastructure Security

Agency (CISA). The meeting took place as organizations continue to address the Log4j vulnerability that has caused concern since it was discovered in December.

Kent Walker, president of global affairs at Google and Alphabet, said that, given the importance of digital infrastructure to the world, it is time to start thinking of it in the same way we do our physical infrastructure.

"Open source software is a connective tissue for much of the online world -- it deserves the same focus and funding we give to our roads and bridges," Walker said.

In a blog post, Walker explained that during the meeting, Google floated several proposals for how to move forward in the wake of the Log4j vulnerability.

Walker said a public-private partnership is needed to identify a list of critical open source projects, and criticality should be determined based on the influence and importance of a project. The list will help organizations prioritize and allocate resources for the most essential security assessments and improvements.

IBM's enterprise security executive Jamie Thomas echoed Walker's comments and said the White House meeting "made clear that government and industry can work together to improve security practices for open source."

"We can start by encouraging widespread adoption of open and sensible security standards, identifying critical open source assets that should meet the most rigorous security requirements, and promoting a collaborative national effort to expand skills training and education in open source security and reward developers who make important strides in the field," Thomas said.

Walker touted the work of organizations like the OpenSSF -- which Google invested $100 million into -- that are already seeking to create standards like this.

He also said Google proposed setting up an organization to serve as a marketplace for open source maintenance, matching volunteers from companies with the critical projects that most need support. He noted that Google was "ready to contribute resources" to the move.

The blog post notes that there is no official resource allocation and few formal requirements or standards for maintaining the security of critical open source code. Most of the work to maintain and enhance the security of open source, including fixing known vulnerabilities, "is done on an ad hoc, volunteer basis."

"For too long, the software community has taken comfort in the assumption that open source software is generally secure due to its transparency and the assumption that 'many eyes' were watching to detect and resolve problems. But in fact, while some projects do have many eyes on them, others have few or none at all," Walker said.

Joe Brockmeier, the Apache Software Foundation's vice president of marketing, said in a statement that there is no single "silver bullet" to solving the security issues inherent to the open source supply chain. He added that "the path forward will require upstream collaboration by the companies and organizations that consume and ship open source software."

Tech giant Akamai, which also had representatives at the White House meeting, backed many of the measures suggested by Google and IBM, adding that governments and the technology community need to build reliable containment plans for when exploits are identified, improve cross-government and industry information sharing when vulnerabilities are first identified and expand government authorization of solutions to increase defenses.

Boaz Gelbord, Akamai chief security officer, told ZDNet that a key takeaway from the meeting was the collective recognition that more needs to be done to support the open source community to thrive within the ever-evolving threat landscape.

"As a prominent supporter of open source and open standards, Akamai sees a specific need for increased information sharing, strong vulnerability management, and building out containment plans to contain the blast radius of attacks," Gelbord said. "We look forward to expanding our efforts in the open source community and contributing to the important next steps coming out of this White House meeting."

26.Researchers May Have A Method to Keep Quantum Information as Safe as Classical Information

by Matt Swayne
https://thequantuminsider.com/2022/01/12/researchers-may-have-a-method-to-keep-quantum-information-as-safe-as-classical-information/

A team of Moscow State University-led researchers have theoretically shown that quantum information can be kept safe from errors just like classical information, according to Quanta Magazine.

The team — led by Pavel Panteleev and Gleb Kalachev of Moscow State University — released its findings in ArXiv, a preprint server.

This could be good news for quantum computing, the researchers report. Information in a quantum computer is subjected to all kinds of environmental noise that can cause errors in the very sensitive quantum states.

In the study, the researchers combined two classical methods and invented new techniques on their own. Prior to this study, most methods to keep quantum information safe from errors could not compete with the reliable and efficient methods of classical computers.

One of the challenges facing engineers is the challenge of increasing qubits without increasing the size and complexity of quantum computers. This research suggests a path forward to maintain quantum data performance stable as the number of qubits increase in a quantum computer. Quantum startups are now hedging that research, like this, could help lead the way to relatively complex, easy-to-maintain devices, relatively speaking.

The work is preliminary and still theoretical, but researchers are intrigued with the possibilities.

"It brings the theoretical quality of these quantum codes to the point that has existed in classical coding for a long time," Naomi Nickerson of PsiQuantum told Quanta Magazine.

27.Indian Researchers Say Cold Atom Spin Coherence Work Could Help Quantum Computing

by Matt Swayne
https://thequantuminsider.com/2022/01/12/indian-researchers-say-cold-atom-spin-coherence-work-could-help-quantum-computing/

Raman Research Institute scientists report that spin coherence in atomic systems may be long-lived even at extremely low temperatures, according to India media sources. The work may open up the path to more efficient quantum computing.

The technique allows the efficient implementation of quantum operations and logic gates that help the system become a better quantum sensor compared to systems with short-lived coherence, the researchers report in Physics Review Research.

In a statement, officials said: "The newly discovered technique can help study the real-time dynamics of quantum phenomena such as quantum phase transitions in a non-invasive manner."

According to the team, spin is a fundamental quantum property of atoms and elementary particles such as electrons and protons. Quantum properties are more easily observed and controlled at colder temperatures. However, because most detection techniques incold atom experiments are destructive and disturbs the atomic sample during detection, measurements of spin at ultralow temperatures are much harder to investigate and dynamic measurements at those temperatures were not available, the team reports.

The scientists said that they measured the properties of spins and lifetime of an atomic spin state with a million-fold improvement in detection sensitivity compared to the existing technology.

Motivation for the work comes from Nobel laureate Sir C.V. Raman's seminal research into light scattering, often referred to as the Raman effect or Raman Scattering.

According to the team, this technology could have some impressive future uses beyond quantum. Devices based on the technique could more precisely detect small magnetic fields, which has important applications in mining and prospecting. The work also has important applications in biomedical imaging, where time-resolved measurements of small magnetic fields are required.

The team was led by Sanjukta Roy, Dibyendu Roy, and Saptarishi Chaudhuri and included doctoral students Maheswar Swar and Subhajit Bhar from RRI. The Department of Science and Technology and Ministry of Electronics and Information Technology supported this work.

28.Capgemini Launches A Dedicated Quantum Lab And Announces A New Agreement With IBM to Advance Industry Applications of Quantum Computing

by Victoire Grux
https://www.capgemini.com/news/capgemini-launches-a-dedicated-quantum-lab-and-announces-a-new-agreement-with-ibm-to-advance-industry-applications-of-quantum-computing/

Capgemini announced today it has set up a dedicated Lab and team of quantum technology experts from across the globe, to develop capabilities and coordinate research facilities aimed at the advancement of quantum technologies and exploration of their potential. In addition to Capgemini's work to explore Quantum Communications and Quantum Sensing, the initiative also includes a collaboration with IBM to help clients build and maximize their engagements in the areas of Quantum Computing.

Capgemini's Quantum Lab (Q-Lab) comprises quantum technology experts and highly-specialist facilities in the United Kingdom, Portugal and India, to harness the potential of quantum technologies. Capgemini's Q-Lab will coordinate research programs to develop business-driven client propositions for sectors most likely to benefit from quantum technologies in the medium future – life sciences, financial services, automotive and aerospace. It will also drive early experiments with clients in their quantum journeys and accelerate the building of in-house skills and capabilities.

This initiative leverages the experience of specialist technical teams within the Capgemini stable who have already built scientific and technology capabilities in quantum, through early experimentation and incubation with clients.

In addition, Capgemini has signed an agreement with IBM to become an IBM Quantum Hub providing its clients access to IBM's quantum computing systems, including IBM's recently announced 127 qubit processor, 'Eagle', as well as to IBM's quantum expertise and Qiskit, IBM's open-source quantum information software development kit. By working with IBM, Capgemini joins more than 170 IBM Quantum Network members, including Fortune 500 companies, start-ups, academic institutions and research labs, all working to advance quantum computing and explore practical applications. Together, IBM Quantum team and clients are researching and exploring how quantum computing will help a variety of industries and disciplines, including finance, energy, chemistry, materials science, optimization and machine learning, among many others. Through this agreement, Capgemini will make it easier for clients to access IBM's licensed technology and provide them with professional services for end-to-end implementation. It is intended to ultimately demonstrate, with prototypes and proofs of concepts, the potential value of leveraging quantum technologies to tackle previously intractable business problems for clients, working towards the implementation of quantum computing use cases.

"Quantum technology will disrupt the way we compute, sense, and communicate, and will create new industries and business models along the way. The launch of our Q-lab tangibly demonstrates our ambition to bring to our clients the most innovative, breakthrough solutions, and to invest in capabilities early on so we can become the leading quantum systems integrator," said Pascal Brier, Chief Innovation Officer at Capgemini and member of the Group Executive Committee. "Our collaboration with IBM will enable us to explore the vast potential of quantum computing, bringing to our clients the top capabilities and skills available in the market today and tomorrow."

"Establishing a quantum industry will require a deep focus on expanding the quantum computing ecosystem across public and private sectors - something IBM cannot do alone," said Jay Gambetta, IBM Fellow and VP, Quantum Computing at IBM. "By working with Capgemini, clients have even more options for hands-on expertise to develop proofs of concepts to explore the potential of quantum computing across a variety of industries and disciplines."

The Q-lab will focus on three areas of value creation for clients:

- Quantum Computing refers to the use of quantum properties to perform computations[1]. Leading application areas are problems requiring complex optimization, simulation, or machine learning. Companies that typically rely on heavy compute facilities, such as molecular design within life science, fluid dynamics in aerospace, or stochastic financial models, will be amongst the first to benefit.

- Quantum Communications involves transmitting and controlling information using the laws of quantum mechanics. Quantum-secure communications could have an immense impact on areas critical to science, industry, and data security. In addition, it is intended to allow clients to access the new realm of possibilities brought by quantum technologies, in particular on confidential computing, data storage and sharing.

- Quantum Sensing refers to the measurement of quantum states, which are extremely sensi-

[1] A quantum computer has the potential to be exponentially faster than the supercomputers used currently, meaning that for complex problems, potentially thousands, or even millions of times faster, and thus permit solving problems which seem intractable with even the fastest classical supercomputers.

tive to disturbance[2]. Quantum sensing underpin advances in everything from medical diagnosis, autonomous transport and intelligent industries. It can help in measuring electric and magnetic fields accurately, measuring physical quantities against atomic properties, and using quantum entanglement to improve sensitivity or precision.

Capgemini has been accelerating the quantum readiness of its clients through consulting, strategic, engineering and algorithmic development solutions, leveraging its Applied Innovation Exchange network and its engineering teams, as well as ecosystem alliance partners and network of peers. The Group was also recently commissioned by the German Federal Office for Information Security, together with Fraunhofer IAIS, to lead a study in Quantum Machine Learning for IT security.

Capgemini is part of IBM's partner ecosystem, which enables partners of all types – whether they build on, service or resell IBM hybrid cloud and AI technologies – to help clients manage and modernize workloads.

29.CISA Alerts Federal Agencies of Ancient Bugs Still Being Exploited

by Ionut Ilascu
https://www.bleepingcomputer.com/news/security/cisa-alerts-federal-agencies-of-ancient-bugs-still-being-exploited/

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has updated its list of known exploited vulnerabilities with 15 new security issues that serve as a frequent attack vector against federal enterprises.

The latest additions vary in terms of severity and disclosure date, some of them being rated as medium risks while others are as old as 2013.

In combination with other factors such as a threat actor's foothold on the network, old and unpatched devices, and/or device exposure on the public internet, the vulnerabilities are a serious security gap and an opportunity for adversaries.

Ancient bugs on the list

CISA compiled the new list after finding evidence that the security issues newly added to the Catalog of Known Exploited Vulnerabilities are used in ongoing attacks.

Of the 15 entries, only four are more recent, from 2021 and another from 2020. The rest are more

[2] Quantum sensors have the potential to provide new data about the world that classical sensors cannot provide. Examples of quantum sensors include atomic clocks, magnetic resonance imaging, electrometers, and magnetometers

than two years old, the oldest of them from 2013 - a bug in the WinVerifyTrust function tracked as CVE-2013-3900, which affects Windows versions starting XP SP2 to Server 2012.

Another aged vulnerability is from 2015, a remote code execution in IBM WebSphere Application Server and Server Hy Server Hypervisor Edition, identified as CVE-2015-7450 and rated as critical (severity level 9.8 out of 10).

The table below shows all the vulnerabilities that CISA wants federal agencies to remediate this month to boost defenses against active threats. CISA recommends applying available updates as per vendor instructions.

.

.

.

CISA's catalog of known exploited vulnerabilities is part of the Binding Operational Directive (BOD) 22-01 for reducing security risks and for better vulnerability management.

Under this directive, federal civilian agencies have to identify in their systems the security issues listed in the catalog, and to remediate them.

Although the catalog is aimed mainly at federal civilian agencies, it is a good reference for organizations of all types to reduce their exposure to cyber risks.

30.9 Ways That Cybersecurity May Change in 2022

by Lance Whitney
https://www.techrepublic.com/article/9-ways-that-cybersecurity-may-change-in-2022/

The dramatic rise in ransomware and other cyberattacks over the past year has finally driven home the point that cybersecurity needs to be taken much more seriously. Amid initiatives by the U.S. government and other parties, there's a growing global awareness of the need to focus on security to combat attacks that threaten vital areas of society. How might this renewed focus on security start to play out in 2022? Ping Identity CEO and founder Andre Durand offers his take with nine cybersecurity predictions for the new year.

- **Cybersecurity will become an ESG issue**

  ESG (environment, social and governance) is a method used by investors and other people to evaluate businesses based on more socially conscious standards. With greater investments in security needed to protect society, cybersecurity will become the fourth responsibility of ESG for corporations, according to Durand.

  "The digital economy has been really important for years, but the pandemic has shifted even bigger parts of our economy to the digital world," Durand says. "We must have appropriate digital identity safeguards in place, or we will have online chaos and fraud running rampant, greatly inhibiting our economic prosperity. Governments need to emphasize and elevate digital security laws and enforcement to the same degree as physical laws and safety are handled today."

- **MFA will become a global mandate**

To better secure logins and protect sensitive data, multi-factor authentication (MFA) will be required not just in the U.S. but around the world, Duran says. As only one of several steps required to improve security, MFA needs to start with key sectors such as government, healthcare, utilities, banking, and education. But consumers will also begin to demand measures like MFA to secure their information and will increasingly desert businesses that fail to take security seriously.

- **Bad bot tsunami**

Malicious bots that impersonate human beings are a threat to customer-facing systems, according to Durand. These types of automated attacks can lead to credential stuffing, account takeovers and account fraud. Sneaker bots can buy up limited inventory of a hot product and then resell them at inflated prices. Traditional security solutions no longer cut it when combating bots, as scammers have learned how to thwart them. Instead, artificial intelligence and machine learning are needed to better distinguish a bot from a human being. And such tools are already here, Durand says. This technology looks for bots by analyzing such factors as how fast a user types, how a user navigates a website or an app and how hard a user presses on a touchscreen.

- **Focus will shift to Zero Trust authorization**

To make sure only the right people have access to the right data, authentication will increasingly shift to authorization, as seen with Zero Trust.

"While it's been trending this way for many years, the corporate network perimeter became a thing of the past during COVID, making Zero Trust authorization more important than ever," Durand says. "While a recent executive order by the Biden Administration is mandating Zero Trust for government entities, we will start to see private enterprises mandate that certain cybersecurity measures are in place in order to do business together."

- **Rise of digital wallets**

People will increasingly store verified data about themselves on their phones, Durand says. As just one example, their real identity will be saved in government-issued IDs through digital wallets provided by Apple and Google. But other types of identity data will be shared with the user for better privacy and control.

There are pros and cons to digital wallets and IDs. On the plus side, they can ensure the identity of the user in business or financial transactions, reduce fraud and identity theft, and shrink the cost and overhead for organizations that typically create physical methods of authentication. On the minus side, a person can be at risk if their mobile device is lost or stolen, a device without power due to an exhausted battery is of little use when trying to present your digital IT, and any digital verification that requires connectivity will fail if there's no cellular or Wi-Fi available.

- **Attacks on zombie and shadow APIs**

Shadow or zombie APIs pose a security risk, as they're typically hidden, unknown and unprotected by traditional security measures. More than 90% of attacks in 2022 will focus on APIs, according to Durand. And for organizations without the right type of API controls and security practices, these shadow APIs will become the weak link.

- **Convergence of IT and OT**

Information technology and operational (physical) technology will collide as IT teams assume responsibility for the security of physical devices. This trend will require interoperability between IT and OT, leading to a convergence of technology to determine who can physically get in a building and who can access key applications. As such, organizations will need universal security requirements of all vendors who are part of the process.

- **Identity focus shifts to user experience**

Amid security changes, user experience must still be considered and prioritized. Customers don't really care about the technical process that occurs behind the scenes, Durand says. Instead, they want a seamless digital experience so they can easily access their accounts and make purchases. Consumer-facing companies that don't offer a smooth user experience will be ditched for companies that do.

- **Rise of the CISO**

As corporate boards increasingly focus on cybersecurity, more people will report directly to the CISO, and the CISO will report to the board, according to Durand. More boards will also set up a dedicated cybersecurity committee by 2025, according to a Gartner forecast.

"CISOs can clearly define tangible risks to the business and present solutions to reduce or completely remove risks to the business that could cause monetary or brand reputation issues," Durand says. "The office of the CISO helps to educate and keep employees fluent and aware of security risks to the business and to themselves. Having the CISO at the right level inside of the company can ensure high and critical security risks are being addressed in a timely manner."

31.Last Year Was A Record Year For At-

tacks, And Log4J Made It Worse

by Jonathan Greig
https://www.zdnet.com/article/report-increased-log4j-exploit-attempts-leads-to-all-time-peak-in-weekly-cyberattacks-per-org/

Cybersecurity firm Check Point Research has released new data from 2021 showing that among their customers, there was a significant increase in overall cyberattacks per week on corporate networks compared to 2020.

Researchers attributed some of the increases, which were concentrated toward the end of the year, to the Log4J vulnerability discovered in December. Check Point said in a report that 2021 was a record-breaking year for cyberattacks and the Log4J vulnerability only made things worse.

"Last year, we saw a staggering 50% more cyber attacks per week on corporate networks compared to 2020 -- that's a significant increase. We saw cyberattack numbers peak towards the end of the year, largely due to the Log4J vulnerability exploit attempts," said Omer Dembinsky, data research manager at Check Point Software.

"New penetration techniques and evasion methods have made it much easier for hackers to execute malicious intentions. What's most alarming is that we're seeing some pivotal societal industries surge into the most attacked list. Education, government and healthcare industries made it into the top 5 most attacked industries list worldwide."

Check Point found that for 2021, overall attacks per week on corporate networks grew 50% compared to 2020, and in Q4, they saw an all-time high in weekly cyberattacks per organization of 925.

Check Point's customers in the education and research space dealt with an average of 1,605 attacks per organization every week, the highest volume of attacks they saw. This represented a 75% increase compared to 2020. The government, defense, military, and communications industries were not far behind, averaging around 1,100 attacks weekly per organization.

When they broke their internal data down by region, they found organizations on the African continent saw the highest volume of attacks in 2021, with an average of 1,582 weekly attacks per organization. Organizations in the APAC region saw an average of 1,353 weekly attacks per organization, while Latin America dealt with 1,118 attacks weekly and Europe saw 670 attacks weekly. North America was last with a weekly average of 503.

Check Point bases its numbers off of its internal ThreatCloud tool that pulls data from hundreds of millions of sensors worldwide.

Dembinsky said he expected the numbers to increase for 2022 as hackers "continue to innovate and find new methods to execute cyberattacks, especially ransomware."

"We're in a cyber pandemic if you will. I strongly urge the public, especially those in the education, government and healthcare sectors, to learn the basics on how to protect themselves," Dembinsky said. "Simple measures such as patching, segmenting your networks and educating employees can go a long way in making the world safer."

32.Cellframe Network: Post-Quantum Encryption And Decentralized Applications

by PR Desk
https://zycrypto.com/cellframe-network-post-quantum-encryption-and-decentralized-applications/

We decided to tell new investors and remind those who came before what the Cellframe Network is, how it works, how it is useful, and whether it will remain secure in the era of quantum computers.

About the project

Cellframe Network is a service-oriented blockchain platform. The project API allows you to develop decentralized applications: auctions, data warehouses, marketplaces, games, and others. The developers focused on quantum security: the Cellframe Network encryption system withstands attacks from quantum hacking algorithms and will remain relevant in the post-quantum era.

The company scales the project using two-level sharding technology when instead of one chain of blocks or events, there are many chains organized according to different rules. The blockchain code is written in C. The peculiarity of this language is high application response speed and low load on the CPU and RAM. All this makes the platform more accessible because the node can be run on weak hardware.

How is Cellframe fundamentally different from other blockchain ecosystems?

The main features of Cellframe are post-quantum encryption and two-level sharding. Multi-Algorithm Signature helps to better protect data from quantum hacking techniques.

At the top level of the shard, parachains arise — independent blockchain networks, with their consensus, but compatible with the rest of the ecosystem and have their level 2 shards inside.

CN is a ready-made solution for business: the blockchain works out of the box and does not require special knowledge from employees. Its extensions can be written in Python, the most popular and simplest language in the world.

Safety

The Cellframe network uses several encryption algorithms at once. The most promising are NewHope, NTRU, Frodo, and SIDH. Another interesting algorithm is Picnic — a Zero-Knowledge Post Quantum

Signature.

Several algorithms help counter different quantum hacking techniques. By default, the network uses the Crystal-Dilithium digital signature, but the user has the option to apply a multi-algorithm signature for greater security.

Scalability

The Cellframe blockchain is split into shards. Sharding helps to distribute the load on servers by parallelizing processes. This approach improves system performance and blockchain throughput. It also solves the problem of horizontal scalability: instead of a single blockchain, we have multiple shard chains.

Each account is tied to a specific shard. The user can join the nearest segment or request the creation of a new one. The segment size is limited, so overflowing shards can deny users' registration. All shard requests are made through messages within the level 0 blockchain. The developers took this step to balance the load on shards (and servers).

Enterprise solution

The project architecture is service-oriented. On its basis, you can easily create second-level protocols with specialized services, and private shards with a built-in payment system make it possible to focus on developing the service.

How the network works

The Cellframe Network ecosystem consists of networks (parachains), the main of which is the Core Network or Backbone. The backbone is arranged like a typical parachain and consists of a zero chain, which is a blockchain common to all shards, and a plasma (DAG, split into shards). In addition, there are also additional sub-chains — support chain common to all, rat chain, linear blockchain flow chain divided into shards, and several others specific to specific Node services registered on the backbone.

Almost all nodes on the network have the same privileges, so the network can be called a peer-to-peer network. The system includes several types of nodes: light, full, archive, master, root. The service node is distinguished separately, which must be the master node on the backbone, but in other parachains, the situation may be different. An important type of service node is the so-called bridge node.

When connecting to the network, the node asks the root for whitelisting the nodes and their IP addresses, pings the nearest ones, and connects to 2-5. Then the first node gives you a new id, which is generated based on the key for it, and the blockchain is synchronized with the nodes.

After that, you can announce your address and supplement the whitelists with the public key of the node, price lists for services, orders, and so on. After verification, the node will be able to share its service and become a master or service node. The main conditions are the availability of this service (Proof-of-Service) as well as the presence of a stack of CELL tokens, own or delegated for a percent-age of profit from services

Network Perspectives

With the development of quantum computers, a large part of the encryption algorithms will become a thing of the past, followed by the cryptocurrencies that used them. A sad fate awaits bitcoin: its digital signatures are based on ECDSA encryption, which is vulnerable to Shor's algorithm. Cellframe Network developers have focused on quantum secure data encryption. Cellframe uses Crystal Dilithium and Picnic signatures.

Dilithium is one of three signature schemes that are considered "finalists" of the NIST standardization procedure; it is built on the problems of lattice theory — MLWE and MSIS. It is believed that either NIST or FALCON will soon be standardized. Dilithium features the smallest public key-signature pair among NIST candidates. Picnic is an "alternate" NIST candidate. Its cipher is not as well understood as AES, however, Picnic keys are much more compact than the latter. Both of these signatures are resistant to Shor's and Grover's algorithms. It means that the platform will remain relevant in the post-quantum era.

33.IBM Welcomes LG Electronics to The IBM Quantum Network to Advance Industry Applications of Quantum Computing

by Elizabeth Banta & SooNa Ryu
https://newsroom.ibm.com/2022-01-10-IBM-Welcomes-LG-Electronics-to-the-IBM-Quantum-Network-to-Advance-Industry-Applications-of-Quantum-Computing

"IBM today announced that LG Electronics has joined the IBM Quantum Network to advance the industry applications of quantum computing.

By joining the IBM Quantum Network, IBM will provide LG Electronics access to IBM's quantum computing systems, as well as to IBM's quantum expertise and Qiskit, IBM's open-source quantum information software development kit.

LG Electronics aims to explore applications of quantum computing in industry to support big data, artificial intelligence, connected cars, digital transformation, IoT, and robotics applications - all of which require processing a large amount of data.

With IBM Quantum, LG can leverage quantum computing hardware and software advances and applications as they emerge, in accordance with IBM's quantum roadmap. By leveraging IBM Quantum technology, LG will provide workforce training to its employees, permitting LG to investigate how potential breakthroughs can be applied to its industry.

"Based on our open innovation strategy, we plan to use IBM Quantum to develop our competency in quantum computing," said Byoung-Hoon Kim, CTO and Executive Vice President of LG Electronics. "We aim to provide customers with value that they have not experienced so far by leveraging quantum computing technology in future businesses."

"We're happy to welcome LG Electronics to a growing quantum computing ecosystem in Korea at an exciting time for the region," said Jay Gambetta, IBM Fellow and VP, Quantum Computing at IBM. "The relationship between IBM and LG Electronics will permit LG to explore new types of problems associated with emerging technologies and will help strengthen the quantum capabilities in Korea."

Quantum computing is an exciting evolution in computation. While classical computers calculate in bits that represent 0 and 1, quantum computers use qubits that harness quantum mechanical phenomena such as interference and entanglement in computation to solve problems that are fundamentally intractable for classical computers. As a result, quantum computing is well suited to help explore new approaches of solving problems like those in LG Electronics' open innovation strategy including big data, artificial intelligence, connected cars, digital transformation, IoT, and robotics applications.

At the IBM Quantum Summit in November 2021, IBM recently unveiled its new 'Eagle' quantum computing processor with 127 qubits, a major step forward in IBM's roadmap to reach Quantum Advantage.

There are more than 170 clients, including LG Electronics, Fortune 500 companies, start-ups, academic institutions and research labs working with IBM Quantum technology to advance quantum computing and explore practical applications. The IBM Quantum team and clients are researching and exploring how quantum computing will help a variety of industries and disciplines, including finance, energy, chemistry, materials science, optimization and machine learning, among many others.

34.Making Next Generation Quantum Computers Even More Powerful

by EPFL
https://scitechdaily.com/making-next-generation-quantum-computers-even-more-powerful/

"IBM and Google currently have the world's most powerful quantum computers," says Prof. Edoardo Charbon, head of the Advanced Quantum Architecture Laboratory (AQUA Lab) in EPFL's School of Engineering. "IBM has just unveiled a 127-qubit machine, while Google's is 53 qubits." The scope for making quantum computers even faster is limited, however, due to an upper bound on the number of qubits. But a team of engineers led by Charbon, in collaboration with researchers in the U.K., has just developed a promising method for breaking through this technological barrier. Their approach can read qubits more efficiently, meaning more of them can be packed into quantum processors. Their findings appear in Nature Electronics.

Biochemistry and cryptography

Quantum computers don't work like the computers we're used to. Instead of having a separate processor and memory chip, the two are combined into a single unit known as a qubit. These computers use quantum properties such as superposition and entanglement to perform complicated calculations that regular computers could never do in a reasonable timeframe. Potential applications for quantum computers include biochemistry, cryptography, and more. The machines used by research groups today have around a dozen qubits.

"Our challenge now is to interconnect more qubits into quantum processors – we're talking hundreds, even thousands – in order to boost the computers' processing power," says Charbon.

The number of qubits is currently limited by the fact that there's no technology yet available that can read all the qubits rapidly. "Complicating things further, qubits operate at temperatures close to absolute zero, or -273.15°C," says Charbon. "That makes reading and controlling them even harder. What engineers typically do is use machines at room temperature and control each qubit individually."

"It's a real breakthrough"

Andrea Ruffino, a PhD student at Charbon's lab, has developed a method enabling nine qubits to be read simultaneously and effectively. What's more, his approach could be scaled up to larger qubit matrices. "Our method is based on using time and frequency domains," he explains. "The basic idea is to reduce the number of connections by having three qubits work with a single bond."

EPFL doesn't have a quantum computer, but that didn't stop Ruffino. He found a way to emulate qubits and run experiments under nearly the same conditions as those in a quantum computer. "I incorporated quantum dots, which are nanometer-sized semiconductor particles, into a transistor. That gave me something that works the same as qubits," says Ruffino.

He's the first PhD student in the AQUA Lab to study this topic for his thesis. "Andrea showed that his method works with integrated circuits on regular computer chips, and at temperatures approaching qubit ones," says Charbon. "It's a real breakthrough that could lead to systems of large qubit matrices integrated with the necessary electronics. The two types of technology could work together simply, effectively and in a reproducible manner."

35.Tech You Need to Know: Homomorphic Encryption

by Ellison Anne Williams
https://www.idgconnect.com/article/3644110/tech-you-need-to-know-homomorphic-encryption.html

Data is at the heart of the digital economy and organisations are constantly on the hunt for better, broader ways to utiliSe their own data — and increasingly, they are also seeking ways to access and leverage data outside their walls. At the same time, a growing heterogeneous regulatory landscape is adding to the complexity of this pursuit by demanding that privacy and security be prioritised.

The need to accommodate both the desire for broader access and restricting regulatory requirements is leading many to explore how technology-enabled solutions can help simultaneously address these challenges. This path frequently leads to homomorphic encryption, a pillar of the Privacy Enhancing Technologies category with the potential to disrupt how and where organisations can leverage data.

What is homomorphic encryption?

By its most basic definition, homomorphic encryption (HE) protects data while it's being used or processed by allowing computations to occur in the encrypted or ciphertext domain. This is different from the more familiar types of encryption that protect data as it moves through the network or while it's at rest on the file system. It can be helpful to think of the distinction between these three states of data — at rest, in transit, and in use — as three points of a triangle. While all are important, Data in Use is the segment that is most frequently overlooked, in part because it's a hard problem to solve but also because, until fairly recently, there was a lack of scalable, practical, commercial-ready solutions.

To help visualise the concept of Data in Use protection, imagine encryption as a vault protecting sensitive data. Traditional practice requires taking data out of the vault every time it needs to be used or processed (to perform a search, apply analytics, evaluate a machine learning model, etc.). This exposure leaves both the data and the operation exposed and vulnerable. HE changes the game by allowing these actions to take place without extracting sensitive data from the protected vault of encryption, as it can also protect the operation and its corresponding results. This ensures sensitive interactions — for example, the interests and intentions of the party performing a search — remain protected throughout the processing lifecycle.

These powerful capabilities have led to HE being referred to as the "holy grail" of cryptography, and they are also why it has been the subject of research and academic pursuit for nearly four decades. Once computationally impractical for use at scale, performance and utilisation breakthroughs over the past several years have prompted increased exploration and adoption in a number of market verticals. And while there continues to be a lot of great progress being made in the academic and research communities, HE has proved that it's now ready for the move to real-world deployments.

The business case for homomorphic encryption

For business users, HE expands the ways organisations can securely share and leverage data to unlock value. For example, HE is being used today to expand the usage and sharing of regulated data across privacy jurisdictions. Utilising HE-powered search capabilities, users initiate an encrypted query in one jurisdiction and searches over data holding in another jurisdiction. The use of HE ensures that any sensitive and/or regulated information contained in search itself — as well as the corresponding results — remain encrypted throughout the processing lifecycle. This enables a decentralised form of data sharing and collaboration as the data remains in each originating jurisdiction and ensures that sensitive data is never exposed outside of the trusted domain in which the search was initiated. For financial institutions operating in jurisdictions around the world, this expanded secure and scalable access allows them to broaden their visibility for use cases such as anti-money laundering, fraud detection, and Know Your Customer screenings.

Other use cases for HE include secure collaboration, third-party risk, and data monetisation. By protecting data while it's being processed, HE enables organisations to use external data assets where they are and as they are today, without exposing sensitive indicators. This ability to collaborate without pooling or centralising data expands the ways in which third party entities can work together as all contributors are able to maintain positive control and ownership of their data assets. The technology also can be configured to continue respecting the access and verification controls established by the data owner. Existing sensitive or regulated data assets can be used in ways that may have previously been determined as too risky to pursue.

While the transition from innovative technology to broad commercial use is rarely straightforward, homomorphic encryption is on its way. The unique capabilities it enables are too transformative to ignore, and it is a technology that will continue to thrive far into the future. By proving its usefulness and impact in real-world use cases today, homomorphic encryption is quickly solidifying its position as a business-enabling, privacy-preserving tool that you need to know.

36.Cybersecurity Training Isn't Working. And Hacking Attacks Are Only Getting Worse

by Danny Palmer
https://www.zdnet.com/article/your-cybersecurity-training-needs-improvement-because-hacking-attacks-are-only-getting-worse/

The threat of cyberattacks is growing and much more needs to be done to educate businesses and users about risks in order to prevent widespread damage and disruption as a result of cyber incidents.

Events like ransomware attacks against utilities and infrastructure providers, production facilities and hospitals have demonstrated that cyberattacks can have very real consequences for people, restricting access to vital goods and services for days, weeks and even months.

But despite the risk posed by cyberattacks, many businesses and their boardrooms still don't fully understand the threats they're facing from cybercriminals and how to best defend their networks against them.

Part of the problem is that, for many businesses, cybersecurity isn't ingrained into everyday operations and employees are only asked to think about it when doing annual cybersecurity training -- leaving companies at risk from cyberattacks the rest of the year.

"I think one of the most important things to realise is most of the education and training done, it's not very effective," Stuart E. Madnick, professor of information technology and engineering systems at MIT Sloan Executive Education told ZDNet Security Update.

"The 30-minute video you're obligated to watch once a year doesn't do the job".

According to Madnick -- who has been at M.I.T. since 1972 and has served as the head of MIT's Information Technologies Group for more than 20 years -- organisations need to build a culture of cybersecurity that actively involves everyone.

If people have a greater understanding of how their organisation falling victim to a cyberattack could affect them, it could lead to everyone being more careful when it comes to cybersecurity.

"If somehow you think you play a role in defending your company, it's important, but that's not something we've been used to in the past, so you have to help people understand that," said Madnick.

Many people associate cyberattacks or being hacked with having their personal information or bank details stolen. But the reality is that cyberattacks are becoming much more damaging and costly. Incidents, from ransomware attacks to data breaches or business email compromise (BEC) scams can cost organisations millions.

And as critical infrastructure and vital services become increasingly connected to the internet, there's the additional risk of cyberattacks causing widespread disruption.

"One thing we're just beginning to see now are attacks on the cyber infrastructure of organisations, like hospitals and power grids," said Madnick.

"Imagine the electricity of London going out, not for an hour-and-a-half, not for a day, but for three weeks. That could be pretty serious," he added, noting this isn't just a fictional scenario, as Ukraine has previously seen power outages in the dead of winter because of cyberattacks, suspected to come from Russia.

That's far from the only time hostile hackers have entered networks of critical infrastructure, with attackers detected inside the networks of American utilities providers. There's the risk that it's only a matter of time before attackers take advantage of vulnerabilities in industrial networks to cause damage and disruption.

If we don't take this seriously we're going to suffer serious consequences, he argues. "That's why it's so important to educate broadly on the implications of
cybercrime," said Madnick.

"The worst is yet to come," he adds, noting how more and more of life now depends on technology.

37.Strangeworks, Quantinuum Work To-

gether On Quantum-Enhanced Cryptographic Key Service

by Matt Swayne
https://thequantuminsider.com/2022/01/05/strangeworks-quantinuum-work-together-on-quantum-enhanced-cryptographic-key-service/

Strangeworks, a global leader in quantum computing software, today announced its latest joint-collaboration with Quantinuum, the largest integrated, stand-alone quantum computing company in the world, with vertically integrated solutions including the highest-performing quantum computer and comprehensive, hardware-agnostic quantum software. This collaboration will implement Quantinuum's quantum-enhanced cryptographic keys, Quantum Origin, into the Strangeworks ecosystem.

Quantum Origin is the world's first commercial product to generate cryptographic keys using quantum computers, and will become an important component of the ecosystem, providing its users seamless access to superior cryptographic keys and helping to protect against current security threats.

"It's fitting that Strangeworks would expand its industry leading platform to include quantum technology to help defend against today's cyber threats," said Duncan Jones, Head of Cybersecurity at Quantinuum and Cambridge Quantum. "We are excited to integrate Quantum Origin to generate the strongest cryptographic keys for Strangeworks and their customers, based on verifiable quantum randomness."

As the world's leading Quantum Service Provider™, Strangeworks is continuously looking at providing their customers and their Quantum Syndicate members the latest quantum-based security offerings, connected through the Strangeworks ecosystem. Due to the variety of quantum systems available and the data sharing of its users, it's important to enable the latest in cybersecurity technology. By implementing Quantum Origin, Strangeworks will be the first to implement a seamless path to quantum-generated cryptographic keys for its quantum computing ecosystem, and expects to expand the relationship between both parties, enabling rapid adoption and insights on how the technology is performing through its productive, yet anonymous, feedback loop.

"We're excited to welcome Quantinuum into the Quantum Syndicate. Expanding our managed quantum services to encompass cyber security is a natural addition to our enterprise offerings," said William Hurley, founder and CEO of Strangeworks. "The integration of Quantum Origin enables enterprises around the world with a seamless path to quantum-generated cryptographic keys to protect their sensitive data."

38.Google's 2021 Year in Review Lays out Hopes for Practical Quantum Computing

This Decade

by Michael Gariffo
https://www.zdnet.com/article/googles-2021-year-in-review-lays-out-hopes-for-practical-quantum-computing-this-decade/

Despite its massive promise, quantum computing is still often seen as a highly-experimental area of tech development that may or may not go anywhere. While Google admits the science behind these almost science-fictional computers has a long way to go, its latest review of its ongoing plans shows a company hoping to turn quantum computing from a nebulous series of promises into a concrete, practical tool in humanity's technology arsenal.

Despite being a retrospective, the main focus of Google's 2021 Year in Review: Google Quantum AI release is the future of the technology. Yes, the company does go over the progress it made during the year in its efforts to build error-free qubits and more practical hardware, but it quickly moves onto its dreams for the still-young 2020s. This long-term commitment, Google said, is focused on three key areas:

- Bringing quantum computing processor technology to the point where it can outperform not only classic computers, but also classic supercomputers.
- Developing a reliable method of error correction for the quantum noise that currently plagues efforts to turn the technology into a practical tool.
- And building a logical qubit that maintains its error-free state for "an arbitrarily long time" to aid in the aforementioned path toward practicality.

The company would like to accomplish all of these things before the calendar rolls around to 2030. Should it attain its goals, Google believes quantum computers could revolutionize multiple areas of technological development. Chief among them is the study of physical systems. The search giant noted in its release that indications of a collaborative study it conducted alongside Caltech show quantum computers can make determinations about physical systems using "exponentially fewer experiments than what is conventionally required." Google also saw similar results when testing the technology's usefulness for chemical engineering purposes alongside Columbia University.

More far-flung applications also include studying the physical oddities of time crystals, calculating statistics for entanglement entropy, and other things that would sound right at home coming out of a Starfleet engineer's mouth.

To help these efforts along, Google reiterated its financial commitment to quantum development, noting it expects to continue expanding its Quantum AI facilities in Santa Barbara, California while also distributing its open-source Cirq quantum computing platform. Other future development plans also include the release of a new Fermionic Quantum Simulator that takes "advantage of the symmetry in quantum chemistry problems to provide efficient simulations," and an update to the qsim tool that allows for the simulation of noisy quantum processors using off-the-shelf GPUs.

39.Cyberattack Against Uk Ministry Of Defence Training Academy Revealed

by Charlie Osborne
https://www.zdnet.com/article/ex-officer-reveals-cyberattack-against-uk-ministry-of-defence-training-academy/

A retired military officer has disclosed a cyberattack that struck the UK Ministry of Defence (MoD) academy and had a "significant" impact on the organization.

Air Marshal Edward Stringer, an officer in charge at the time, told Sky News that the cyberattack was discovered in March 2021.

According to the retired officer, "unusual activity" was detected by IT outsourcer Serco but originally it was thought that this may have been due to some form of IT error rather than something malicious.

The Defence Academy of the United Kingdom was the target. The organization is responsible for teaching and training thousands of military personnel, MoD employees, wider government figures, and overseas students. Courses on offer relate to topics including security, strategy, languages, and information warfare.

While full attribution is not available as to whom was responsible, the publication reports that China or Russia was "possibly" involved.

Iran and North Korea were also floated as potential sources of the cyberattack.

"It could be any of those or it could just be someone trying to find a vulnerability for a ransomware attack that was just, you know, a genuine criminal organization," Stringer said.

As academy staff worked to keep courses running, management was concerned that the reason behind the attack may not have been to disrupt the educational system - but rather, the academy could have been used as a "backdoor" to target the wider MoD. This prospect had severe ramifications and could have had potential consequences for national security.

Stringer added that despite these concerns, there appears to be no evidence of breaches beyond the Defense Academy.

An investigation has been launched and the National Cyber Security Centre (NCSC) is aware of the cyberattack.

During the interview, Stringer said the cyberattack was "significant, but then manageable" - and further prompted the academic institution to ramp up its security posture and network resiliency after accounting for the "operational cost" of dealing with the incident.

As of now, the IT infrastructure is still being rebuilt and the Defence Academy is set to launch a new website in the future.

An MoD spokesperson told Sky News:

"In March 2021 we were made aware of an incident impacting the Defence Academy IT infrastructure. We took swift action and there was no impact on the wider Ministry of Defence IT network. Teaching at the Defence Academy has continued."

40.New Standards Rolling Out for Clocking Quantum Computer Performance

by Charles Q. Choi
https://spectrum.ieee.org/quantum-computer-benchmarks

For conventional computers, benchmarks can represent a rite of passage of sorts into a new era of computing. As artificial intelligence and machine learning become more and more ubiquitous, for instance, AI and ML benchmarks help everyone understand and measure precisely how well one neural net performs compared to other systems as well as to reference architectures. Not surprising, then, that the emerging field of quantum computer benchmarking will be helping test and improve next-generation quantum processors, researchers say.

A quantum computer with great enough complexity—for instance, enough components known as quantum bits or "qubits"—could theoretically achieve a quantum advantage where it can find the answers to problems no classical computer could ever solve. In principle, a quantum computer with 300 qubits fully devoted to computing (not error correction) could perform more calculations in an instant than there are atoms in the visible universe.

However, researchers at Sandia National Laboratories note that it is currently difficult to accurately predict a quantum processor's capability—that is, the set of quantum programs it can run successfully. This is because the current benchmarking programs used to analyze these devices scale poorly to quantum computers with many qubits. Existing quantum benchmarks are also not flexible enough to supply detailed looks on processor capabilities on many different potential applications, they say.

"It's surprisingly difficult to benchmark state-of-the-art quantum computers, because most benchmarks rely on comparing the results of a quantum computation with the correct output, computed on a conventional computer," says study lead author Tim Proctor, a physicist at Sandia National Laboratories' Quantum Performance Laboratory in Albuquerque, New Mexico. "That conventional computation becomes utterly infeasible as the number of qubits increases, which was central to Google's famous 'quantum supremacy' demonstration."

The new benchmarks detail a quantum computer's performance on different tasks—compared to existing standards that generate just one number.

In a new study, Proctor and his colleagues developed a novel technique for creating benchmarks for quantum computers that they call circuit mirroring. This method transforms any quantum program into an ensemble of closely related benchmark programs dubbed "mirror circuits," which each perform a set of calculations and then reverses it.

The mirror circuits are each at least as difficult to execute as the quantum program they are based on. However, unlike many quantum programs, mirror circuits have simple, easy-to-predict outcomes. As such, mirror circuits provide a way to verify a quantum processor's capabilities using benchmarks similar to quantum programs the quantum computers may actually run, the researchers say.

"Quantum computers are complicated, and quantifying their performance is complicated too. Our methods can be used to design benchmarks for studying all kinds of aspects of a quantum computer's performance," Proctor says. "Ultimately, we think that benchmarks built using our method could be used to design a set of comprehensive tests for quantum computers. This would make it possible to accurately compare quantum computers, and to find out which hardware is best for which task."

Using circuit mirroring, the scientists first designed two families of benchmark programs—one that ran quantum processors through randomized sequences of operations, the other with highly structured procedures. They next executed these benchmarks on 12 publicly accessible quantum computers from IBM and Rigetti Computing to map out their capabilities.

Quantum benchmarking currently relies mostly on randomized programs. However, Proctor notes such randomized benchmarks may not serve as well as tests of the more structured programs that quantum computers employ to implement quantum algorithms.

A competing standard, cycle benchmarking, is customized to each algorithm—and measures error rates for sets of quantum gates.

Indeed, Proctor and his colleagues found that how well quantum computers executed randomized mirror circuits did not predict how well they did with more orderly mirror circuits. The performance of some quantum processors depended heavily on the level of mirror circuit structure, while others showed almost no sign of such a link.

"A particularly nice feature of our benchmarks is they're designed to provide a lot of detail—they tell us about a quantum computer's performance on different tasks," Proctor says. "This contrasts to most existing methods that, by design, describe a quantum computer's performance with one number."

One potential flaw of benchmarks that employ the reversal technique used in mirror circuits is how they may fail to detect many key errors. "We ensure that our benchmarks are sensitive to all errors by inserting a random element in between the forward and reverse circuits, the two parts that comprise the bulk of a mirror circuit," Proctor says. "In the paper, we prove that our benchmarks are sensitive to all errors." The scientists detailed their findings Dec. 20 in the journal Nature Physics.

41.Quantum Resistance: Taking Proof Of Keys Day To The Next Level

by Jameson Lopp
https://bitcoinmagazine.com/culture/proof-of-keys-day-and-quantum-computing

When Satoshi Nakamoto mined the genesis block 13 years ago today, giving rise to the Bitcoin blockchain, he sparked a cryptographic revolution — you could store your wealth behind personal private keys.

Recognized every January 3, Proof Of Keys Day is an opportunity to reflect on that breakthrough by ensuring that you hold your private keys. In recent years, Bitcoiners have celebrated this day by taking their bitcoin off of exchanges.

At Casa, we help Bitcoiners take self custody of their keys, and we've found that some education is required to use this power effectively. This year, we're taking Proof Of Keys Day a step further by calling out a threat on the horizon and explaining why we should act now to keep our keys as robust as ever. That threat is quantum computing.

What Is Quantum Computing?

You may have noticed that computers are a lot smaller than they used to be. This is the result of countless scientific breakthroughs, ranging from nanophysics to the chemistry of semiconductor materials. In quantum mechanics, we're studying the world at the most granular level possible to unlock the potential of base materials and complex applications.

Quantum computing is where the fields of quantum mechanics and computer science meet. As our atomic and subatomic understandings grow, we apply this knowledge to create more powerful and efficient computers.

We are living in the Information Age. Those who wield the best technology will reap massive rewards in the years to come. It's hard to envision the potential of quantum computing because we don't know what we don't know. Building a quantum computer is like trying your hand at alchemy or cold fusion — if you somehow manage to succeed, the payoff could be limitless.

What constitutes quantum computing is hard to describe comprehensively, but for the sake of argument, consider it a transcendental improvement to processing power, far bigger than 10 times or 100 times improvement. Quantum processing power is measured in qubits. It's thought that certain types of Bitcoin addresses could become susceptible to attack at several thousand qubits, and the latest advanced model is around 125 qubits. So, while quantum computing isn't a phenomenon we expect in the immediate future, it's within a couple of orders of magnitude, which may not be very long in technological terms.

Peace Through Superior Firepower

Cryptography allows us to obscure information into a format that is practically impossible to guess or compute, and cryptography is what makes Bitcoin highly defensible. The software clients and wallets can change — the cryptography must remain intact.

Each Bitcoin address is generated with a private key, a number so cosmically huge that it's difficult to comprehend. It's like a lock with nearly infinite combinations. A malicious actor could try to guess your private key, but they would most likely die of old age trying.

Processing power is important from a game-theoretical perspective because computers continue to advance every year, as predicted with Moore's law. Bitcoin only survives as long as the potential for a computational attack against public keys remains out of reach.

To date, no one has been able to accomplish such a feat, but this is not guaranteed to always be the case. Cryptographic algorithms do tend to get weakened and eventually cracked as our understanding of math and computing evolves.

Satoshi's First Line Of Defense

Satoshi anticipated continued technological advancement to some extent. They included one safeguard to keep actors from overtaking the Bitcoin network with processing power alone: the difficulty adjustment. The algorithm self-regulates every 2,016 blocks, increasing or decreasing mining difficulty to keep the relative time for Bitcoin blocks at roughly every 10 minutes.

This dynamic feature was a must-have in Bitcoin's early days when the network was at its most vulnerable and wild hash rate changes posed an existential threat. For the most part, the difficulty adjustment has encouraged those who briefly gain a computational advantage to use their power for good and mine bitcoin, rather than attack the network.

There is, however, the theoretical possibility of a massive computational breakthrough that imbues a corporation or nation state with a lopsided advantage over the network. To get an idea of the scale we're talking about, consider how the development of the nuclear bomb tipped the scales of World War II. If an actor were to ever obtain such an advantage, they are heavily incentivized to deploy it right away, rather than watch it fade slowly over time.

Upgrades Will Be Necessary

If a quantum computing attack occurred, some network components would be more vulnerable than others. For instance, there's often discussion about whether Satoshi's coins — an amount estimated to be as high as 1.1 million bitcoin — will ever move. But the more alarming scenario could be if Satoshi's coins were stolen.

Early Bitcoin addresses are weaker from a cryptographic standpoint. These addresses use a pay-to-public-key (P2PK) set up, meaning the actual public key can be found on the blockchain. A powerful enough quantum computer could potentially reverse engineer a private key from a public key and spend from the associated address. This means Satoshi's coins could become "mineable" if the coins stay put for all eternity and quantum computing arrives.

Most addresses in recent years use a pay-to-public-key hash function, which provides another layer of cryptographic protection, but the scenario mentioned above illustrates how problematic the right kind of supercomputer can be. Attackers look for the weakest link as a point of entry.

The Future of Bitcoin Is Quantum Resistance

Computation is competition. While the quantum computing threat is not something we expect to be worth worrying about for many years, it is better to be proactive rather than wait for it to come for us. Security is the science of staying ahead. The very act of wealth preservation is comprised of staving off the many attempts to steal it.

One immediate strategy for personal quantum resistance is to never reuse addresses. Once you spend from an address, you expose the address' public key on-chain. By withholding your public keys, you make it harder for a quantum computer to eventually target you with reverse engineering. This is a tactic that you can use today.

Going forward, we Bitcoiners should engage in continual discussion on how to upgrade our cryptographic infrastructure to prepare for the rise of quantum computing because — let's face it — we know it's coming. The recently activated Taproot upgrade, which eschews the participation of multiple signatures behind a single one, is a good example of what can be accomplished if we put our minds together. We can harness the innovation of quantum computing for the good of Bitcoin.

Proof Of Keys Day is more than a one-day affair — it's a way of life. As Bitcoiners, it's up to prove our keys time and again in the face of evolving threats. Cypherpunks write code and they never stop writing.

42.Ten Cybersecurity Resolutions For a Safer 2022

by Jamilah Lim
https://techwireasia.com/2022/01/ten-cybersecurity-resolutions-for-a-safer-2022/

New year, new resolutions — here are ten cybersecurity practices we think that you and your business need to usher a safe and cyber-secure 2022 in.

(i) Prioritize cybersecurity

A TrendMicro **survey** found that 90% of IT decision-makers claim their business would be willing to compromise on cybersecurity in favour of digital transformation, productivity, or other goals. 82% also felt that they have been pressured to downplay the severity of cyber risks to their board.

Whilst a data breach might make organizations prioritize cybersecurity, the costs of handling one would be immense — we're talking **US$5 million per breach** immense.

Why would you buy umbrellas after the rain?

(ii) Don't neglect data protection and privacy

Customers say that **safety and security are most important to them** online. KPMG suggests that businesses adopt a transparent approach to how data is used, stored, and shared. This will not only assuage the worries of users but also help to build consumer trust in a brand.

Don't betray their trust, ensure you have the right **data protection** and **data privacy** policies in place within your digital ecosystem.

(iii) Institute and maintain IT and cybersecurity hygiene policies

Ransomware will be the largest threat to businesses this year. Sophos recommends having proper IT hygiene policies across the company.

Ensure **proactive countermeasures** such as monitoring features, backups, and training in security skills to enable early detection. Ensure all staff has the latest security updates and patches installed on their devices.

(iv) Passwords are not enough

Eighty percent of hacking-related breaches can be attributed to weak or compromised passwords, according to Verizon's 2019 Data Breach Investigations Report.
So, passwords aren't enough. Multi-factor authentication (MFA) should be the new norm.

(v) Zero-trust is your friend

Yes, we've said this ad nauseam. We're saying it **again**. And **again**.

(vi) Beware tech support scams

Over 60% of consumers around the globe have **fallen prey to tech support scams.** Victims tend to be younger men, and also very overconfident of their IT literacy skills.

So what should businesses do? Consider AI chatbots instead for tech support.

(vii) Prioritize 5G security

5G technology is gaining increased uptake in the Asia Pacific and will see more use in 2022. However, it does come with security concerns, especially as it may enable a wider threat surface area for attackers.

As such, it's time to prioritize 5G security both **MNO-side** and **business side.**

(viii) Increase remote working security

We thought remote working would be decreasing. Boy, were we wrong, especially given the rapidly spreading Omicron variant.

Companies should continuously implement and reinforce **user-friendly cybersecurity tools and policies**, and users should improve on their security standards at home.

(ix) Break IT team silos down

Only a third of developers truly understand the security policies they work with. This disconnect between security teams and software developers hinders initiatives like Zero Trust implementation and securing the cloud.

Companies should **foster closer relationships** between developers and the security team so all ICT members are on board and fully understand how policies and processes will be like.

(x) … or outsource IT security

Well, if your company is smaller and you can't afford a security team, then **cybersecurity MSPs** (managed service providers) are a solution.

But make sure you get the advice of a skilled and experienced cybersecurity member to ensure you're not overpaying for services you don't need.

43.Quantum Technology: How It Works, Applications And Why The Us And China Are Racing To Achieve Supremacy

by Dylan Dean
https://www.scmp.com/news/china/science/article/3161830/quantum-technology-how-it-works-applications-and-why-us-and

In November, the United States government added 12 more Chinese companies to its export blacklist, citing national security concerns. This time, quantum computing firms were among them.

According to the US Commerce Department, some of the firms added to the blacklist aided the Chinese military's "counter-stealth and counter-submarine applications, and the ability to break encryption or develop unbreakable encryption".

These are all applications that have been linked to quantum technology, which both the US and China are racing to develop.

How exactly does this technology work, and is it really a game-changer?

What is quantum technology?

Quantum technology is a complicated area of physics that explores the behaviour of subatomic particles – particles that are smaller than atoms, the basic building blocks of all matter.

One major area of interest within quantum technology is quantum computing. Unlike a classic computer, which performs calculations one at a time, a quantum computer can perform many calculations at the same time.

The basic unit of information in classic computing is a "bit", which represents one of two binary values – either zero or one. The computer is able to interpret these values and represent them in various formats, including words and images.

Quantum computers use a different basic memory unit: a qubit, which has the flexibility to represent either zero, one or both at the same time. This ability of an object to exist in more than one form at the same time is known as superposition.

Things get more complicated when multiple qubits in the computer interact with each other.

This is where the concept of entanglement comes in: multiple particles in a quantum system are connected and affect each other.

For example, if one qubit represents zero, another qubit entangled with it will assume the value of one, and vice versa, making the measurement of each qubit dependent on the other.

Because quantum computers' basic information units can represent all possibilities at the same time, they are theoretically much faster and more powerful than the regular computers we are used to. Physicists in China, for instance, recently launched a quantum computer they said took 1 millisecond to perform a task that would take a conventional computer 30 trillion years.

If they're so great, why aren't all computers quantum computers?

Considering our obsession with speed in technology, you might think quantum computing would be the default by now.

But so far, these machines work only in a protected environment for short periods on highly specific tasks, and they make a lot of mistakes. Hence, it is a matter of debate between scientists whether "quantum supremacy" – the idea that quantum computers could do better than their conventional counterparts, at least on some specific tasks – has ever been achieved.

One big challenge for scientists is getting qubits to maintain superposition and entanglement long enough to complete a task. Quantum states of superposition and entanglement are extremely fragile and without the right temperature and environmental conditions, they lose their qualities quickly and behave erratically.

To function properly, qubits have to be stored in special refrigerators at ultra-low temperatures close to the point where atoms stop moving. The need for specialised equipment is a key reason only countries willing to invest a large amount of resources have studied quantum computing.

Leading Chinese quantum physicist Pan Jianwei estimated in October it would take "four to five years of hard work" to correct quantum errors for two quantum computers his team developed, before they could look at solving important scientific questions with practical value.

What are some potential applications?

In an article published in 2020, Pan, the father of China's quantum satellite programme, outlined three applications for quantum technology the country was trying to develop:

(i) **Quantum sensors** which could reveal a submarine hiding hundreds of metres under the ocean, or guiding devices that could operate independently for months without a GPS signal.
(ii) **Quantum computers**, which could perform calculations that would take present-day high-performance computer thousands of years to solve – such as cracking encryption – in seconds;
(iii) **Quantum internet** using entangled particles to transmit messages, leading to ultra-secure communications.

Aside from military and national security applications, quantum research could help achieve important scientific breakthroughs.

There are hopes that quantum computing could help researchers develop new drugs by modelling larger, more complex molecules a lot faster, according to a 2021 McKinsey report.

Researchers are also studying climate applications, and propose that high-speed quantum computing simulations could help scientists create more efficient batteries or fertilisers, or find ways to optimise processes to reduce carbon emissions.

As interest in quantum computing applications grows, tech giants at the front of R&D – including IBM, Google, Huawei Technologies Co. and the South China Morning Post's parent company Alibaba – have provided free platforms for people to develop quantum algorithms.

Which countries are leading in the quantum technology race?

Britain, the European Union and the US have all published plans in recent years to take a lead role in the global race on quantum science and technology.

China's national quantum programme, on the other hand, was shrouded in secrecy until 2020, when it listed quantum technology as a top priority, along with six other key science and tech areas in the country's five-year development plan.

In December 2021, a Harvard report said that in quantum computing, quantum communication and quantum sensing – three areas traditionally led by US researchers – "China is catching up and, in some cases, has already overtaken America".

Both countries have invested a huge amount of money and set out stringent policies related to the study of quantum technology.

In September 2020, Pan and his team claimed to have achieved quantum supremacy with a new machine that was one million times faster than the record held by Sycamore, a quantum computer built by Google.

China has more than 3,000 patents related to quantum technology, about twice as many as the US, but falls behind in terms of patents specific to quantum computing, according to a Valuenex report in 2021.

Why is the US worried about China's quantum research?

According to a US congressional research report, quantum computing could be a threat to current encryption methods by around 2030-2040.

Modern encryption used to protect information is nearly impossible for regular computers to crack, but quantum computers could do so with their superior processing power.

This could allow "adversaries to gain access to sensitive information about US military or intelligence operations", the report said.

The report also predicted that with improvements in both quantum computing and machine learning, a subfield of artificial intelligence, countries could develop more accurate and deadly weapons.

China has already developed quantum equipment with potential military applications.

This year, scientists from Tsinghua University developed a quantum radar that could detect stealth aircraft by generating a small electromagnetic storm.

In 2017, the Chinese Academy of Sciences also developed a quantum submarine detector that could spot submarines from far away.

44.Quantum Computing in 2022: A Leap Into The Tremendous Future Ahead

by Samhitha
https://www.analyticsinsight.net/quantum-computing-in-2022-a-leap-into-the-tremendous-future-ahead/

Quantum computing has progressed from an experiment to a tool to an apparatus that is now making advances in the venture to tackle complex issues. Experts accept that the world has gone into the 'Quantum Decade' — an era when ventures start to see quantum computing's business esteem. The advances in equipment, software development, and administrations approve the technology's momentum, which is making it ready for additional breakthroughs in 2022 and helps the market for the inevitable reception of this revolutionary technology.

What is quantum computing's fate in 2022? Or is it capable enough to turn our fate all around? We at Analytics Insight brought a quick synopsis of quantum computing's predictions and performance in 2022.

The Quantum Race is in Underway.

Governments worldwide have resourced more than US$25 Billion to quantum research and development. Tech giants like IBM, Google, Alibaba, Microsoft Amazon, and different organizations are in the competition to adapt quantum computing as an ordinary tool for business.

IBM for instance pronounced its plans to assemble a 1,000-qubit quantum computer by 2023, a very first time in the tech business, and furthermore broke new grounds in November by revealing 'Eagle', a cutting-edge processor that is apparently the most remarkable quantum computing processor created by IBM thus and could pioneer a notable new path in IT. Letters in order have assembled a 54-qubit processor Sycamore and exhibited its quantum matchless quality by playing out an errand of creating an irregular number in 200 seconds, which it cases would take the most exceptional supercomputer 10,000 years to do the responsibility. The organization likewise disclosed its most up-to-date 72-qubit quantum computer Bristlecone. Alibaba's cloud administration auxiliary Aliyun and the Chinese Academy of Sciences mutually sent off an 11-qubit quantum figuring administration, which is accessible to general society on its quantum computing cloud platform

Not simply big technology companies, well-funded start-ups have likewise designated the quantum computing space to develop hardware, algorithms, and security applications. Some of them are Rigetti, Xanadu, 1Qbit, IonQ, ISARA, Q-CTRL and QxBranch. One of the significant objectives organizations are as of now making progress toward is purported quantum incomparability, when a quantum computer plays out an estimation that no traditional computer can act in a sensible measure of time. In October 2019, Google additionally asserted it arrived at quantum matchless quality, however, this case was questioned. A few specialists, similar to Intel's head of quantum hardware, Jim Clarke, imagine that the genuine objective ought to be "quantum practicality" he told IEEE, alluding to the moment that quantum computers can really accomplish something changing and unique. Furthermore, researchers accept that gradually and consistently quantum computers will walk into the enterprise domain doing things that would have been generally unthinkable.

An Ocean of Opportunities for Enterprises

The different analyses and drives with quantum computing by the big tech and other organizations are setting out an ocean of open doors before CIOs and IT offices to apply the innovation into this present reality settings. Quantum computers are undeniably appropriate for settling complex optimization- and performing quick quests of unstructured data, as Prashanth Kaddi, Partner, Deloitte India makes reference to, "it can possibly bring problematic change across areas, including finding, medication research, dispersion store network, traffic flow, energy optimizing and many more.

Quantum computing additionally fundamentally diminishes time to market, just as helps in enhancing customer delivery. For instance, a drug organization may essentially decrease an opportunity to showcase new medications. In finance, it could empower quicker, more complicated Monte Carlo stimulations, like trading, trajectory optimisation, market instability, and value advancement procedures, and some more.

Once more, JP Morgan Chase and Co alongside IBM is creating further developed philosophies for monetary demonstrating including choice estimating and risk analysis. Another firm, ExxonMobil plans to settle the strategic difficulty of moving the world's cleanest-consuming fuel LPG across the globe in association with IBM Quantum.

Further, Mitsubishi Chemical is applying quantum computing to assist foster lithium-air batteries with more noteworthy energy density in organization with IBM Quantum. IBM and the University of Tokyo formed the Japan – IBM Quantum Partnership, a broad national partnership framework in which other universities, industry, and government can engage.

This way, quantum computing has a future full of possibilities, opportunities in the digital spectrum. Putting it in a nutshell, 2022 is going to be the year of quantum computing.