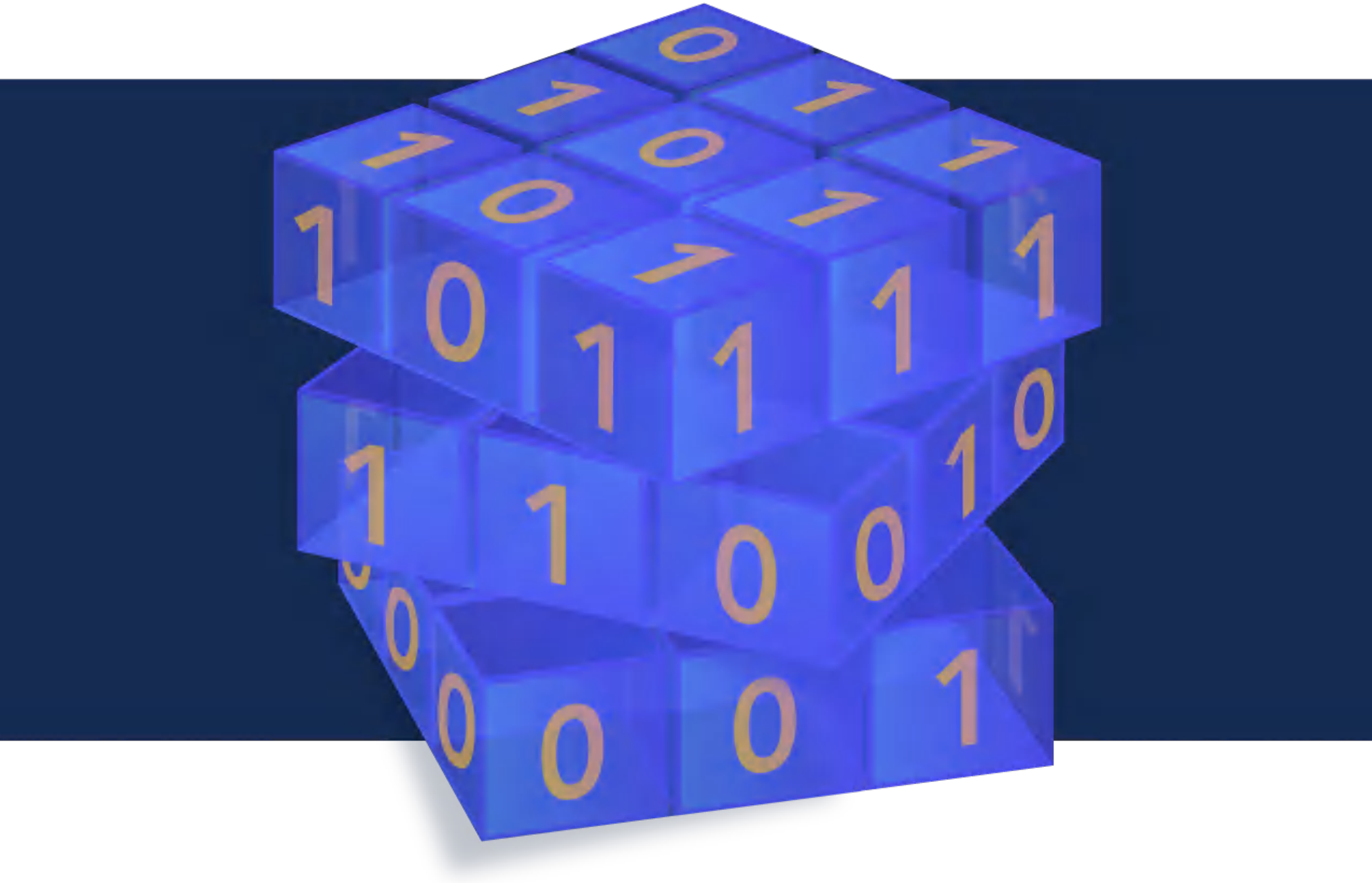
Crypto News

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

July 01, 2022



1. Editorial

It's time for this month's Crypto Newsletter! Let's start with a question. Have you heard of the EU proposal to outlaw encryption? Yes … really! It's being proposed as a part of the new "protect the children" bill. Take a look at article #9 for more information and how certain countries are not on board with enacting this piece of legislation. For our history buffs, check out article #14 to learn more about Alan Turing's contributions to general computing, artificial intelligence, and cryptography. In the mood for more international news? If your organization has operations in India or route any data through the country, you should navigate to articles #29 and #38. They explain in detail the new guidance set forth by CERT-Ins. There is pushback from tech policy groups but companies may have no choice but to comply with the guidance despite their misgivings about them. Last but not least, make your way down to article number #40. Get your answers from NIST Theorist Alexey Gorshkov on what's so great about quantum computing. There is even more intriguing content in this issue so make sure to skim through. 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.

2.ARSAT developed CryptoComm, a post-quantum cryptographic security system

by Bnamericas

https://www.bnamericas.com/en/news/arsat-developed-cryptocomm-a-post-quantum-cryptographic-security-system

State telecommunications company Arsat, worked with Argentine cryptographers to develop an inviolable communications system for messages and files based on post-quantum methods (PQC), called CryptoComm, to provide protection for many years. Its objective is to create systems resistant to quantum attacks.

The development was explained during the Seminars on Secure Communications led by Arsat's general management attaché, Dr. Hugo Scolnik, in a live chat via videoconference, which was presented by the company's CEO, Matías Tombolini. State agencies, private companies and interested individuals learned about CryptoComm and have even advanced in the request to install the software in the activity in which more than 250 people participated over two days.

The existence of quantum computers and their enormous associated capacity threatens to destroy confidentiality both on the internet and in digital signature structures. The vulnerabilities would primarily affect asymmetric methods (RSA, ElGamal, Elliptic Curves, DSA, etc.) but would also affect symmetric algorithms such as AES by reducing the complexity of brute force attacks.

The method developed consists of a high-speed symmetric cipher (with 318-bit keys), which can be used effectively in communication systems. They also implemented a new post-quantum technology for generating private/public keys and digital certificates.

There are two versions: The "S" version system allows the exchange of files and messages through software. Then the "H" version will be launched, which will implement the system through specialized hardware developed between Arsat and Invap. Additionally, the functionality of real-time voice and video transmissions will be added.

It is clear that given the growing evolution in the development of quantum computers, this threat is no longer virtual and it is necessary to adopt this technology to protect our communications and the assets of the country, the only way to build Cybersecurity and National Cyberdefense. That is why, currently, to implement a secure communications system, it must be done with post-quantum methods.

The truth is that it is useless to resort to physical and logical resources from abroad since there are countless examples of hidden back doors that violate that security. That is why Arsat is investing in national human resources to meet the challenge.

3.Research award establishes sole-source provider of post-quantum cryptography for agencies

by Dave Nyczepir
https://www.fedscoop.com/sbir-post-quantum-cryptography/

The Small Business Innovation Research program awarded **QuSecure** a Phase III contract, establishing the company as the sole-source provider of post-quantum cryptography for more than a dozen federal agencies Wednesday.

QuSecure is the first quantum security-as-a-service company to achieve Phase III, intended to commercialize its software solution, QuProtect, which uses quantum-resistant cryptography to protect communications and data on any device. There is no cap on Phase III funding, with the average winner receiving more than $100 million in 2021.

SBIR made the award to hasten agencies' adoption of post-quantum cryptography, after National Security Memorandum-10 gave them a year from the day algorithms are approved to release transition plans. Agencies are concerned that China and other nation-states are developing quantum computers capable of breaking the public-key cryptography that secures most federal systems.

"We want to work with as many [agencies] as we possibly can," Pete "Shadow" Ford, senior vice president of federal operations, told FedScoop. "They're calling."

The SBIR agencies are the Small Business Administration; departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Transportation; Environmental Protection Agency; NASA, and the National Science Foundation.

QuSecure is in talks with various Commerce agencies, DHS and the Department of Justice; is working through clearances with DOD and the Office of the Director of National Intelligence; and has agreements with several National Laboratories, Ford said.

The company's goal is to meet agencies' "basic" post-quantum cyber needs to start — providing each with solutions at the appropriate technology readiness level (TRL) — as it continues to work its way up the NASA-developed scale on its way toward protecting top-secret data enclaves, Ford said.

What solutions agencies need this fiscal year depends on their individual use cases and implementation timeframes.

"The Department of Justice may need something completely different, as part of their risk management framework for vulnerability, than, let's say, a DOD customer," Ford said. "And NASA may need something completely different for exoatmospheric than other customers that are indoatmospheric."

QuSecure received SBIR Phase I funding, which goes up to $250,000, in 2019 and Phase II funding, up to $1.25 million, earlier this year — a testament to the speed of its Phase III award. The company only stood up federal operations in January.

Phase III also allows QuSecure to receive subcontracts and funding outside SBIR, and it can win future Phase III awards when practical.

The company is emphasizing crypto-agility, the ability to work with multiple post-quantum cryptography algorithms, as the National Institutes of Standards and Technology prepares to approve several for standardization in the next few weeks.

"Are you able to work with all?" Ford said.

4.CERT-In extends new privacy rules for VPN providers to September 25

by Tech Desk

https://indianexpress.com/article/technology/tech-news-technology/cert-in-extends-new-privacy-rules-for-vpn-providers-to-september-25-7996158/

The Indian Computer Emergency Response Team (CERT-In) has given Virtual Private Network (VPN) providers and cloud service operators an extension of three months to comply with its newly drafted VPN rules. This comes as VPN providers such as SurfShark, NordVPN, and ExpressVPN **removed their India servers** citing a threat to the anonymity and privacy of users.

However, the deadline now has been extended to September 25, the Ministry of Electronics & IT (MeitY) said in a press statement.

On April 26, CERT-In had **asked VPN service providers** to maintain for five years or longer details such as the validated names of their customers, the period for which they hired the service, the IP addresses allotted to these users, the email addresses, the IP addresses and the time stamps used at the time of registration of the customers. It also wants VPN service providers to maintain data such as the purpose for which the customers used their services, their validated addresses and contact numbers, and the ownership pattern of the customers.

The ministry's cyber-arm in an order stated that it is extending the timeline for implementation of these Cyber Security Directions upon several requests of micro, small and medium enterprises (MSMEs). It also received multiple requests from VPN, Data Centres, Virtual Private Server (VPS) providers, and Cloud Service providers.

Meanwhile, the government is fixed on its stance on the new VPN rules. CERT-In has in its April 26 directive also said that these details are necessary to prevent incitement or commission of any "cognisable offence using computer resources or for the handling of any cyber incident" which may lead to any disturbance in the "sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order".

Earlier last month, Minister of State for Electronics and Information and Technology Rajeev Chandrashekhar warned VPN companies that if they do not adhere to the norms, they are free to exit the country. "If you're a VPN that wants to hide and be anonymous about those who use VPNs and you don't want to go by these rules, then if you want to pull out (from the country), frankly, that is the only opportunity you will have. You will have to pull out," he said.

5.Cyber and post-quantum era

by Kirsi Kokko
https://www.professionalsecurity.co.uk/news/interviews/cyber-and-post-quantum-era/

A golden era of quantum technology is coming tantalisingly close. It promises to carry the baton for powerful high-speed processing and sophisticated cyber security solutions that could shake up the future of computing.

Quantum computers are processors that have the capability to solve complex calculations in hours that would take years in classical computing not rooted in quantum physics. As Germany's Federal Office for Information Security (BSI) has advised that a cryptographically relevant quantum computer will be available by 2030, the dawning of the quantum age is just around the corner.

Unfortunately, such computing power also has the potential to give cyber criminals access to computers forceful enough to crack what we think of as our most secure digital encryption. Hackers with quantum tools would be able to open and read in the future any data stolen today - including financial transactions and government communications.

That means there is an urgent need to start developing innovations to secure the internet and all forms of exchanged data and communications from present and future post-quantum threats.

A giant leap for industries

Quantum computing technology represents a giant leap for industries such as healthcare, space research, finance, and online security. Information that used to take months or years to generate will soon be available in an instant.

The global quantum computing market is forecast to grow dramatically over the next 10 years. By 2023, 76% of high-performance computing centres worldwide are forecast to be using quantum computing — the majority with an on-premises infrastructure. But, as the cost of building a quantum computer falls over the next ten years, the entire world's data will become vulnerable to theft and exploitation.

The race is therefore on to develop and update our encryption technologies so that they are equally challenging for classical and quantum computers before it is too late to protect data and organisations from the threat of attacks.

The need for quantum cyber security

This will drive the need for post-quantum cryptographic solutions to provide the most effective and efficient security capable of protecting communications systems and preventing quantum computing-related hostile intrusion.

And it is a priority for nations around the world. The US, is already pushing ahead with security technology as President Joe Biden recently signed an executive order to support quantum technology aiming to head-off adversaries who use the next generation of super computers. He will also sign a national security memorandum outlining the administration's plan to address the risks posed by quantum computers to America´s cybersecurity infrastructure.

Meanwhile, in the UK, demand for cyber security to protect the future of the financial services sector, the largest in Europe, is high. According to a study supported by the UK Foreign Office, 78% of regulators identify cyber security as the biggest area of risk for financial services and the National Cyber Security Centre has also issued advice to UK businesses to prepare for a step-change in cybersecurity technology brought about by more widespread access to quantum computers.

Here, Finland has had a head start on the race to create post-quantum cryptography technology thanks to financial investment and business incentives from the Finnish Government. As a result, some of the first innovators to develop cyber security solutions have come from business in Finland, who are now calling on the tech community to join their mission to protect our post-quantum world.

Developing ground-breaking solutions for a quantum era

Following more than £3m in investment from the Digital Trust initiative, the Post-Quantum Cryptography (PQC) project, led by VTT (Finland's Technical Research Centre) is one such organisation leading the way with some of the world's first quantum-secure encryption technologies.

It aims to be ready for the new quantum era by developing cryptography knowhow and skills as well as and best practices for certification of post quantum products and services. It's already on that journey thanks to work collaborating with the National Institute of Standards and Technology (NIST) to produce Post-Quantum Cryptography Standardization – quantum resistant cryptographic algorithms for new public key crypto standards set to be released in 2023-25.

This research is essential, as one of the most worrying applications of quantum computing is its potential for breaking the public-key RSA algorithm – which secures the nearly $4 trillion ecommerce industry. While it would take a classical computer trillions of years to break RSA encryption, a quantum computer could defeat RSA in hours.

Further Finnish organisations, including SSH, Bittium and Insta, are among the first to explore solutions to protect such data in transit by encrypting file transfers and securing remote access with post-quantum technology, as well as quantum encryption that can secure Ethernet and IP traffic across any network, to ensure it remains safe in the quantum computing world.

But more cybersecurity solutions are needed to protect the world from the growing numbers of quantum computers we expect to see in the next 10 years. And to achieve that, more technology innovators need to join the mission to secure our post-quantum world.

Only the finest minds will do

As the technology industry looks to the post-quantum cryptography (PQC) age, adopting cyber security innovation is essential for all organisations. But the world first needs more innovative providers of quantum computing security solutions to protect businesses from potential hacks and attacks.

That requires the finest minds in the quantum technology worldwide. Collaboration and global partnerships are essential to deliver innovation that will harness the potential of quantum technologies as well as protect the threats posed by quantum technologies.

Science transcends borders, and cooperation with partners accelerates the way we bring technologies to market. The current geopolitical situation and war in Ukraine emphasise the need for European sovereignty and partnerships between like-minded countries, researchers, and companies to develop innovations and solutions to keep us safe. Innovators like PQC aim to be ready for the new quantum era by developing cryptography knowhow. But to ensure the post-quantum future is safe for us all, more companies need to join the call to collaborate with the Finnish quantum crypto community and develop quantum level cybersecurity tools to protect us all from potential hacks and attacks.

The brave new world of quantum computers is almost here. Now is the time for businesses like yours to join the community currently funding innovations and developing international market-ready tools. The technology community needs to start developing cyber security innovations that will allow the world to take full advantage of the opportunities quantum technologies will bring to benefit society and the economy at large.

We cannot afford to wait, the time to act is now.

6.What is Quantum Key Distribution (QKD) & Who's Involved in 2022?

by James Dargan
https://thequantuminsider.com/2022/06/28/what-is-quantum-key-distribution-qkd-whos-involved-in-2022/

According to The Quantum Insider's proprietary data platform, there are some thirty companies exploring Quantum Key Distribution (QKD) as a technology.

But what is this technology and how does it work?

One of the fundamental building blocks of encryption is key distribution. This allows cryptographic keys to go from one party to another (or vice versa) for encryption and sharing in a secure fashion.

The basis of current systems (public-key cryptography) in securing key exchanges is good, old-fashioned mathematics. Unfortunately, these can be compromised by advances in technology such as better computational processing power, more modern hacking methods and weak random numbers.

And this scenario is only set to get worse with the advent of fault-tolerant quantum computers.

Unlike traditional encryption methods, however, QKD leverages physics to pass on keys between two parties.

Any attempts to eavesdrop or even intercept the key will—due to the fundamental laws of quantum mechanics, where measuring the quantum system disturbs it, ultimately breaking it and deeming it unhackable—guarantee its security.

QKD is information-theoretic secure. This means that even with the unlimited processing power available, no black hat operators can break the protocol, deeming the QKD protocol is a secure system, even against quantum computers.

Let's now look at ten of the companies exploring QKD to make the world a more secure place for our data. One more thing, this list is non-exhaustive – Toshiba is a notable omission and we haven't covered the national QKD and networking intiatives. If you wish to see other players on the market, please sign up to our quantum market data platform, the leading provider of information, data, and insights on Quantum Technologies market around.

You can also check out our Quantum Security Market Report, available here. This explores the current state of the art and explains why many companies are currently more focused on Post Quantum Cryptography (PQC).

1. **Laser Components**
   Günther Paul founded Laser Components in the West German town of Gröbenzell, back in 1982.

   With headquarters in Olching, Germany, the company specializes in optoelectronic and fibre optical technologies though markets some of its products as being relevant for QKD.

2. **ID Quantique**
   ID Quantique provides multiple quantum cryptography solutions for data protection, with a particular focus on QKD, Quantum Random Number Generators (QRNGs) and is also tracking with interest Post-quantum Cryptograghy (PQC) too.

   ID Quantique is a Swiss company. Based in Geneva, Switzerland and founded in 2001 by Nicolas Gisin, Hugo Zbinden and current CEO and founder Grégoire Ribordy as a spinoff of the Group of Applied Physics at the University of Geneva, it is one of the oldest pure-play quantum companies in the world.

3. **Ki3 Photonics Technologies**
   Ki3 Photonics Technologies is a spinoff company from the National Institute of Scientific research — Energy, Material, and Telecommunication (INRS — EMT). Based in Montreal, Canada, it was founded in 2015 by Yoann Jestin and Piotr Roztocki.

   The company's mission is to improve the accessibility of the QKD technique and it aims to lead the transformation of quantum photonics into an accessible mass technology and develop quantum tools inherently compatible with communications networks.
   As well as developing technology in quantum photonics, Ki3 Photonics also offers hardware and security solutions to protect internal and external communication networks.

4. **KETS Quantum Security**
   Building communications systems using quantum states of light allows dramatic performance advantages over conventional systems, KETS Quantum Security provides a number of technology offerings including on-chip QKD.

In 2018 KETS was named the UK's Most Innovative Small Cyber Security Company at Infosecurity Europe and was a finalist in the Best Tech Startup category and the Business Leader Go: Tech Awards.

Based in Bristol, UK, KETS was founded in 2016 by Jake Kennard and Chris Erven.

5. **Quantum Technologies Laboratories**
   Quantum Technologies Laboratories (qtlabs) develops designs and prototypes for the technical implementation of quantum encryption into its customers' infrastructure, with a particular focus on Space and Terrestrial QKD.

   The Vienna-based quantum communication and cryptography startup was founded in 2017 by Thomas Scheidl, Fabian Steinlechner, Sam L. Tschernitz, and Rupert Ursin.

6. **QNu Labs**
   QNu Labs is developing technologies to make encryption future-proof. Along with products in QRNGs and Post-quantum cryptography, QNu Labs' Armos QKD protects critical infrastructure unconditionally, providing quantum resilience to ensure data in transit is safe at all times.

   Based in Bengaluru, India, the company was founded in 2018 by Sunil Gupta, Srinivasa Rao Aluri, Mark Mathias, and Anil Prabhakar.

7. **Quintessence Labs**
   Quintessence Labs offers various QC security solutions. Its focus has been on QKD and it is expanding its suite of products around this.

   Founded in 2008 by Vikram Sharma and with headquarters in Canberra, Australia, QuintessenceLabs' QKD product, qOptica™ 100, uses lasers to encode the signal enables high throughputs, is compatible with current telecommunication technologies and the ability to use standard fibre connections allows for cost-effective systems, has the ability to use COTS components and integrated functionalities—allowing for reduced form-factor, power, weight and cost—and, finally, can operate unimpaired in daylight conditions, without any filtering.

8. **LuxQuanta**
   LuxQuanta focuses on developing QKD systems and technologies and to distribute cryptographic keys between users with the highest level of security. The result is a technology capable of providing high-performance and cost-effective quantum cryptography solutions, easy to integrate into existing optical network infrastructures while capable of delivering a quantum-safe layer of security on top of traditional cryptographic techniques.

   A spinoff founded in 2021 by Valerio Pruneri and Sebastian Etcheverry from ICFO, The Institute of Photonic Sciences (a world-leading research centre on photonics and quantum technologies)—where it was incubated for over four years—from its headquarters in Barcelona, LuxQuanta's goal is QKD systems and technologies to be integrated into existing network infrastructures while capable of delivering a quantum-safe layer of security on top of mathematical cryptographic techniques.

9. **QEYnet**
   QEYnet is a Toronto-based startup working on a microsatellite-enabled quantum key distribution network.

   Founded in 2016 by spacecraft engineers and quantum communication experts who have built their careers designing low-cost, high-performance spacecraft and ultra-robust QKD technology, respectively, QEYnet is led by Dr. Thomas Jennewein from the University of Waterloo's Institute for Quantum Computing.

   With all this in place, then, the startup's combined experience, network partnerships, licenses, and IP position offer first-to-market space-based QKD, using novel techniques, at a disruptive cost.

10. **ThinkQuantum**
   Last but not least we have ThinkQuantum, a spinoff of the University of Padua, Italy, founded in 2021 by Paolo Villoresi and Giuseppe Vallone.

   Manufacturing QKD distribution platforms, as well as Random Number Generators, ThinkQuantum offers a reliable European supply network and covers the full value chain, from design and manufacturing to commissioning of QKD systems and QRNG devices. Its applications range from ICT and TLC networks, banks, insurance companies and data industries, to providers of security systems services demanding the highest security standards for multiple applications (Computation, Automotive, Professional & Consumer Electronics, etc.), as well as the New Space Economy.

7.Security experts urge agencies to test post-quantum cryptography algorithms now

by Dave Nyczepir
https://www.fedscoop.com/agencies-should-test-post-quantum-algorithms/

Agencies should test post-quantum cryptography algorithms with their software and decide whether information security benefits outweigh the efficiency losses ahead of a federally mandated transition, according to security experts.

Experimenting with the National Institute of Standards and Technology's candidate algorithms, some of which will be standardized, will help agencies understand their impacts on system performance and behavior and craft required plans identifying where to deploy them first.

NIST expects to publish approved algorithms "potentially within a few weeks," a spokesperson told

FedScoop, and while the standards will be optional, agencies may mandate them in accordance with National Security Memorandum-10. The memo requires agencies to inventory their high-value assets and systems vulnerable to quantum computers which, while a decade or more away, will be able to break most public-key cryptography securing systems, and it gives them a year from NIST's release to issue plans to transition to quantum-resistant cryptography.

"The challenge that chief information security officers face is that they eventually have to migrate everything in their organizations onto these new algorithms," said Duncan Jones, head of cybersecurity at Quantinuum.

CISOs must prioritize areas where the data is particularly valuable and the encryption most at risk, and a lot of them don't have that information readily available, Jones said.

Quantinuum released a post-quantum standardization guide for CISOs earlier this month, which wasn't supposed to beat NIST's standards, originally expected out at the end of March, to publication. The guide recommends CISOs begin speaking with vendors about their plans for adopting post-quantum algorithms and refer to the Open Quantum Safe project, which provides a variety of implementations, for experimentation.

"Everyone needs to figure out now if it makes sense to pay the cost at the moment to upgrade to these quantum algorithms, what to prioritize doing sooner rather than later," said Mark Zhandry, senior scientist at the NTT Research Cryptography & Information Security Laboratories. "That can start now; there's no reason to wait for any decisions from NIST."

Foreign adversaries are intercepting communications now and storing them for decryption by a quantum computer, in the next decade or so that it takes to develop one. Agencies need to decide if they're willing to accept any efficiency losses that come with adopting algorithms with substantially larger cryptographic keys, strings of bits used by the algorithm to transfer plain text into cipher text and back, when the threat may be decades away.

For that reason agencies' adoption of NIST's standards will probably occur more slowly when securing less-sensitive information, Zhandry said.

NIST's candidate algorithms are all grounded in "reasonably well-understood" security principles, and no "significant" vulnerabilities have been found, Zhandry said. Once NIST decides on approved algorithms, standardizing them will take 12 to 18 months — likely taking the process into 2024.

The final seven algorithms skew "heavily" toward one type of math, which is "a bit risky" if it's cracked, Jones said. But industry hasn't pushed for any algorithms outside of the finalists it helped develop, and NIST's project, begun in 2016, can always diversify algorithms in future guidance, said the agency's spokesperson.

"This is a big milestone," the spokesperson said. "It's taking slightly longer than we anticipated to announce the first algorithms selected, but we are still on track to have the first post-quantum cryptography standards published by 2024."

8.Dozens of cryptography libraries vulnerable to private key theft

by Ben Dickson

https://portswigger.net/daily-swig/dozens-of-cryptography-libraries-vulnerable-to-private-key-theft

A poor implementation of Ed25519, a popular digital signature algorithm, has left dozens of cryptography libraries vulnerable to attacks.

According to Konstantinos Chalkias, a cryptographer at MystenLabs who discovered and reported the vulnerability, attackers could exploit the bug to steal private keys from cryptocurrency wallets.

Some but not yet all of the vulnerable technologies have been patched.

Where's your Ed at?

Ed25519 is often used as a modern replacement for the Elliptic Curve Digital Signature Algorithm (ECDSA). Ed25519 is more open, secure, and faster than ECDSA, which is why it has become very popular in many sectors, especially in blockchain and cryptocurrency platforms.

"The main benefits against ECDSA is that EdDSA sig[nature]s are deterministic and users don't need [access to] a secure Random Number Generator [RNG] to sign a transaction," Chalkias told The Daily Swig. "Why is this useful? because a user's laptop or IoT device might not have a good source of entropy or support a weak RNG function."

Numerous security incidents have shown that poor random generation can result in private keys being leaked or stolen. One notable example was the private key leaks of PlayStation 3, whose technology relies on the ECDSA algorithm.

Pre-computing public keys

The standard specification of Ed25519 message signing involves providing the algorithm with a message and private key. The function will use the private key to compute the public key and sign the message. Some libraries provide a variant of the message signing function that also takes the precomputed public key as an input parameter. There are some benefits to this implementation.

"Recomputing the public key each time would result in a slower algorithm (it adds an extra scalar to elliptic curve point multiplication to derive the public key, which reduces the speed by almost 2x, potentially making it even slower than ECDSA)," Chalkias said.

"And generally, in cryptography, it's good hygiene to avoid accessing the private key many times. If we allowed the public key derivation on each signing invocation, then this implies we need to access it twice, once to sign, and once to derive the public key."

However, the modification also creates a security loophole in the library.

Chalkias found that some libraries were allowing arbitrary public keys as inputs without checking if the input public key corresponds to the input private key. This shortcoming means that an attacker could use the signing function as an Oracle, perform crypto-analysis and ultimately get at secrets. For example, an attacker who can't access the private key but can access the signing mechanism through an API call could use several public keys and messages to gradually build up insights into private key parameters.

Libraries at risk

Chalkias initially found 26 libraries that were vulnerable to the attack. The list was later extended to 40 libraries. The security researcher also found several online services that were vulnerable to the same kind of attack, including a fintech API.

"In some applications when `keyGen` fails or a clean-up process deletes the `privKey` for this user, then the app usually retries `keyGen`. But in the meantime and for a few sec[ond]s, the DB [database] still stored the old `<userID, pubKeyOld>`, and this allowed a narrow window for race condition attacks before the DB gets updated with the new `pubKey` (a scenario that, surprisingly, we managed to exploit with significant probability)," Chalkias noted.

Since his report, several libraries have implemented fixes and workarounds, including ed25519-elisabeth, PASETO, and Trezor wallet.

"A few libraries [have] already provided either fixes (if they were vulnerable) or proactively added extra checks that the stored pub key corresponds to the private keys," Chalkias concluded.

9.Germany Says "Hell, No" To EU Proposal To Outlaw Encryption

by Mike Masnick
https://www.techdirt.com/2022/06/27/germany-says-hell-no-to-eu-proposal-to-outlaw-encryption/

Last month, we noted that there was a new "protect the children" bill that was proposed in the EU that would **effectively outlaw encryption**, while simultaneously require full internet scanning of basically all activity.

As we noted in our post, it was still early in the process, and now the German government has stepped up to say that this proposed regulation **is a terrible idea and would devastate basic human rights**. That's exactly right.

The German government in the past weeks repeatedly slammed the bill as an attack on privacy and fundamental rights, with its digital minister Volker Wissing warning this week that the draft law "crosses a line."

In response, the EU Commissioner who is championing the proposal tried to insist that the proposal is much more narrow than people are making it out to be, but that's wrong. It's based on the faulty assumption that you can magically keep end-to-end encryption while simultaneously be able to scan messaging communications for certain content. That's not possible.

Hopefully that puts a quick end to this proposal, but I fear it will keep popping up quite a bit over the next few years.

10.Researchers crack MEGA's 'privacy by design' storage, encryption

by Charlie Osborne
https://portswigger.net/daily-swig/researchers-crack-megas-privacy-by-design-storage-encryption

MEGA claims that its storage service is private by design, but according to researchers, the technology is beset with "serious" security issues.

Based in New Zealand, MEGA is a cloud storage service and messaging platform that offers end-to-end encryption to more than 250 million users. MEGA also allows users to make audio and video calls.

The company calls itself a "zero-knowledge" encryption service built with "privacy by design".

"All your data on MEGA is encrypted with a key derived from your password; in other words, your password is your main encryption key," the organization says. "MEGA does not have access to your password or your data."

However, according to the ETH Zurich University, based in Switzerland, in-depth testing of the platform has revealed "security holes that would allow the provider to decrypt and manipulate customer data", despite its marketing claims to the contrary.

ETH Zurich cryptography researchers Matilda Backendal, Miro Haller, and Professor Kenneth Paterson analyzed MEGA's source code and cryptographic architecture, uncovering a total of five vulnerabilities.

Encryption cracked

After recreating part of the MEGA platform and attempting to brute-force their own accounts, the team says they found that using one main key represents a "fundamental" weakness in the service.

A paper (PDF) describing the flaw says that the MEGA client derives an authentication key from a user's password. This key is then used to encrypt other key material, files, and more.

A lack of integrity protection of ciphertexts containing keys breaks the confidentiality of the master key and overall encryption system, according to the researchers. This permits integrity attacks, RSA key and plaintext recovery attacks, and establishes an RSA decryption attack vector.

By hijacking only a session ID, it takes a maximum of 512 login attempts to break into a MEGA account.

"An additional manipulation of the MEGA software program on the computer of the victim can force their user account to constantly log in automatically," the researchers said. "This shortens the time needed to fully reveal the key to just a few minutes."

It then may be possible to compromise other keys used on the MEGA platform.

Potential post-attack vectors could include stealing user data or even uploading files – such as illegal or compromising images and video – locking up the account, and then blackmailing the targeted individual.

MEGA response

Paterson said the team reported its findings to MEGA on March 24 and proposed ways to resolve the security holes.

While MEGA apparently "decided to react in ways that are different than what we suggested," according to the researcher, the initial attack vector on the RSA key has now been patched.

When approached for comment, MEGA pointed us toward a security advisory which says the first fix has been rolled out and additional patches are being developed.

According to MEGA, only customers that have logged into their account at least 512 times could be at risk – and this does not include resuming existing sessions.

Furthermore, the organization says that to take advantage of the cryptographic flaws, attackers would need to "gain control over the heart of MEGA's server infrastructure or achieve a successful man[ipulator]-in-the-middle attack on the user's TLS connection to MEGA".

"The reported vulnerabilities would have required MEGA to become a bad actor against certain of its users, or otherwise could only be exploited if another party compromised MEGA's API servers or TLS connections without being noticed," the firm added.

The Daily Swig passed on this reaction to researchers at ETH Zurich who responded by saying MEGA had only resolved some of the security shortcomings that they had identified:

- As detailed on the webpage of the paper [1], we contacted MEGA on March 24, 2022, to inform them of the vulnerabilities. They responded the same day and acknowledged the issues. They have been very open and communicative throughout. As part of our disclosure, we provided them with three sets of countermeasures, ranging from 'immediate' to 'recommended'.

- MEGA decided to go with a different patch, which protects against the first three out of our five attacks. You can read more about this in their blog post [2]. We continue to stand by our recommended countermeasures, which we believe would protect against our attacks (and others) in a more robust way than the fix that MEGA decided for.

11.How Quantum Computers Break Encryption

by Frank Zickert

https://www.nist.gov/blogs/taking-measure/alan-turings-everlasting-contributions-computing-ai-and-cryptography

Modern asymmetric encryption builds upon the assumption that it is practically impossible to find the prime factors of very large numbers.

Accordingly, the outcry was great when Peter Shor presented his algorithm that allows a quantum computer to factorize a large number efficiently. Of course, we all want to understand how this algorithm works. But unfortunately, it is not exactly beginner-friendly.

Fortunately, we don't need to master factorization to understand how quantum computers break encryption. Instead, we can first use a more straightforward example to understand it conceptually.

Suppose we have a three-character binary message (e.g., 000, 001, 010, 011, etc.) that we want to encrypt and a three-character binary secret — the password, if you will.

We encrypt the message by calculating modulo two of the inner product of the message and the secret key.

The inner product is formed by multiplying the digits at each position and summing the results.

Finally, modulo denotes the remainder of the division of two numbers. So if we divide the inner product by two (modulo two), the remainder is either 0 (if the sum is even) or one if the sum is (odd).

This is our encryption mechanism. It is not as sophisticated as modern asymmetric encryption algorithms but sufficient for explanatory purposes.

The crucial feature of asymmetric encryption is that it consists of two keys: a public key and a private key. We use the public key to encrypt messages and the private key to decrypt them.

Modern asymmetric encryption uses large half prime numbers as public keys and their prime factors as secret keys.

We think this is secure because the number of trials needed to find the prime factors of a number grows exponentially with the size of the number.

So even if someone has the public key, they cannot derive the private key from it. Therefore, we can share this public key with anyone.

In our example case, the secret binary string is the private key. We use a black-box function as the public key. This function uses the private key and the encryption algorithm to generate the encrypted message.

We need to derive the private key solely by using the function to crack the encryption.

In the previous post, we learned that we need to use the function three times to find the secret key.

This is because the inner product multiplies the individual digits independently at each position. Furthermore, it only outputs one if both characters in the corresponding position are one. So by choosing input strings that contain only a single one, such as 001, 010, and 100, we can effectively test whether the secret is a one at the respective position.

Of course, this encryption is so bad that we don't need quantum acceleration to crack it. But let's assume, for the sake of understanding, that it would be too hard. Suppose we needed too many executions to infer the secret key because that is precisely the obstacle that prevents us from breaking factorization-based algorithms. The number of executions simply grows too fast with the size of the secret, exponentially so.

So we need to reduce the number of applications of the public key function and infer the secret key. This is where a quantum algorithm comes into play.

Our algorithm consists of five parts:

1. a set of qubits in superposition in the |+> state, where each qubit represents a digit.

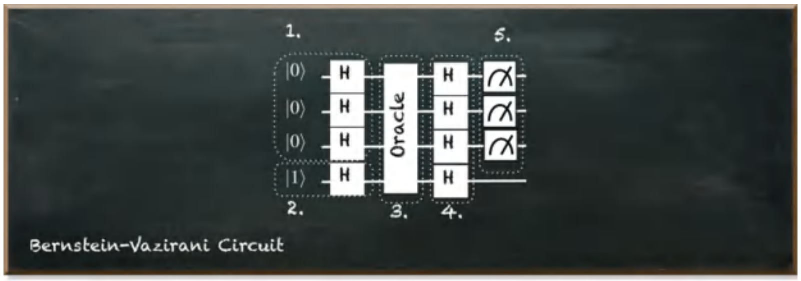
2. an auxiliary qubit in the state |->.

3. a quantum oracle representing the secret key

4. bringing the qubits out of superposition

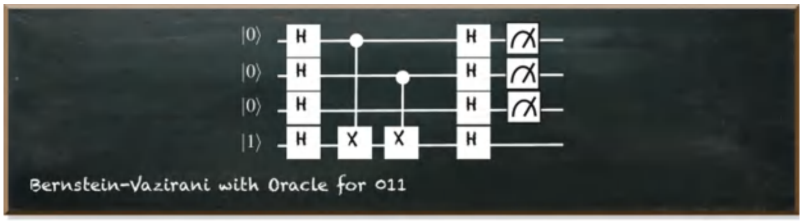
5. measurement of the qubits

The following figure depicts these parts of the algorithm. It is the Bernstein-Vazirani algorithm.



The oracle consists of a controlled X-port (or CNOT) for each 1 in the secret string, with the qubit representing the digit as the control qubit and the auxiliary qubit as the target.

Suppose our secret key is 011, then the complete circuit looks like this.



When we measure the qubits, we see that the qubits representing the digits reveal the secret key by running the entire circuit only once instead of three times as the classical algorithm requires.

12.NRL Announces the Washington Metropolitan Quantum Network Research Consortium (DC-QNet)

by Paul Cage
https://www.nrl.navy.mil/Media/News/Article/3060477/nrl-announces-the-washington-metropolitan-quantum-network-research-consortium-d/

To advance quantum network capabilities and leadership, the U.S. Naval Research Laboratory (NRL) announced work with five other U.S. Government agencies on May 18 to establish the Washington Metropolitan Quantum Network Research Consortium (DC-QNet) to create, demonstrate and operate a quantum network as a regional testbed.

Quantum networks, an emerging research frontier, will one day offer the ability to distribute and share quantum information securely among quantum computers, clusters of quantum sensors and related devices at regional and national distances. They can also be used to distribute ultra-precise time signals, and offer the potential to enable the creation of new applications not yet imagined.

"These agencies with world-class research capabilities will work to advance quantum network capabilities and leadership," Gerald Borsuk, Ph.D., DC-QNet Executive Director said. "Quantum networks will be essential to modern secure communications and to computing enhancements in the 21st Century."

The six agencies are:

- U.S. Army Combat Capabilities Development Command Army Research Laboratory
- U.S. Naval Research Laboratory
- U.S. Naval Observatory
- National Institute of Standards and Technology
- National Security Agency/Central Security Services Directorate of Research
- National Aeronautics and Space Administration

There are currently two out-of-region affiliates to this Consortium:

- U.S. Naval Information Warfare Center Pacific
- U.S. Air Force Research Laboratory

The exploitation of quantum-entangled particles (including photons) to transmit information in the form of qubits, the basic unit of information in quantum technologies, is at the heart of quantum networks.

Quantum entanglement is a unique quantum mechanical property of atomic and subatomic particles, where classical physics fails to describe observed phenomena accurately. It describes a relationship between particles whereby the quantum state of each particle cannot be described independently of the state of the others, even though they are physically separated from each other.

DC-QNet researchers are also studying other quantum behaviors and capabilities such as transduction, or the process of converting qubits from one form into another. To fully harness these capabilities for quantum networking will require state-of-the-art measurement science, or metrology.

The DC-QNet testbed will perform entanglement distribution of qubits at multi-kilometer distances over a well-characterized and controlled quantum network. Efforts include:

1. Development of high fidelity quantum memory nodes, single-photon devices, network metrology, qubit platforms, transduction and frequency conversion, synchronization, and continued research and development into enabling science and technology
2. Developing the network infrastructure to connect the six metropolitan agencies
3. Research and development into the transfer of quantum entanglement between nodes
4. Emulation, modeling and simulation of the network
5. Research and development into the classical management and control, routing, monitoring and metrology and associated software of the quantum network.

The DC-QNet governance comprises an Executive Director and an Executive Steering Committee, along with principal investigators from among the agencies taking the lead on the various technical goals. Among the programmatic goals of the consortium are:

1. A trusted Quantum Network Testbed for the U.S. Government and the U.S. Department of De-

fense

2. Contributions to network synchronization by official U.S. government timekeepers
3. A focus on the metrology required to operate a quantum network

13.What Reaching 20 Qubits Means for Quantum Computing

https://www.honeywell.com/us/en/news/2022/06/what-reaching-20-qubits-means-for-quantum-computing

In the coming decades, more businesses are expected to harness the power of quantum computing to solve complex challenges in cybersecurity, finance, life sciences, logistics and sustainability – problems that increasingly need to be solved with technology more powerful than a classical computer.

Global quantum technology funding and investment activity surpassed $1.4 billion in 2021, more than double that of 2020, according to McKinsey & Company.

Quantinuum, formed in 2021 by the combination of Honeywell Quantum Solutions and Cambridge Quantum, aims to accelerate the development of quantum computing and deliver real-world applications powered by quantum.

Quantinuum's latest milestone: its H1-1 quantum computer expanded from 12 to 20 fully connected qubits and increased the number of quantum operations that can be completed in parallel.

Here's what you need to know.

What 20 qubits means

A qubit – short for a quantum bit – is the smallest unit of data in quantum computing. Unlike the smallest unit of data in classical computing – which is called a binary digit or bit, which exist in either an off (zero) or on (one) position – qubits can exist as zeros and ones simultaneously. That's one ability of quantum computing that makes it more powerful than classical computing.

So, for researchers using the H1-1quantum computer, the upgrade from 12 to now 20 fully connected qubits to run more complex calculations than previously possible without sacrificing performance.

The upgraded system has already been put to use. In a private preview of the H1-1 quantum computer, JP Morgan Chase was able to use the computer to produce an algorithm for Natural Language Processing: a field of artificial intelligence aimed at training computers to comprehend words and conversations like humans. Their results were posted in a pre-print publication to arXiv.

What other quantum applications are being explored?

In parallel with advancing the H-series hardware capabilities, Quantinuum also develops the software and algorithms to be used on quantum computers. Quantinuum recently announced the release of their new Quantum Chemistry software package, InQuanto. In a collaboration with Honeywell PMT, Quantinuum is using InQuanto to explore how quantum computing could aid in the development of new, low global warming potential (GWP) refrigerants.

Cybersecurity is another area in which experts are looking to harness the power of quantum, and Quantinuum's platform Quantum Origin allows the generation of cryptographic keys from the H1 quantum computer that offer superior protection against rapidly advancing cyber threats.

What's next for quantum?

Quantinuum's hardware development has used a unique product strategy of continuously upgrading their hardware after initial product release, concurrent with customer usage. The recent upgrade of H1-1 to 20 qubits was an example of such an upgrade. And similarly, the second version of the System H1 machine, H1-2, is slated to undergo similar upgrades later in the year.

Quantinuum also is developing its next-generation hardware technologies, which include more complex trap designs and other upgrades that will enable the company to bolster computational capabilities. All align with the hardware technology roadmap that Quantinuum has made publicly available.

14. Alan Turing's Everlasting Contributions to Computing, AI and Cryptography

by René Peralta

https://www.nist.gov/blogs/taking-measure/alan-turings-everlasting-contributions-computing-ai-and-cryptography

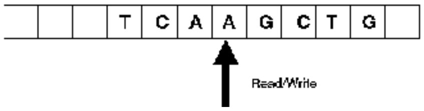
Suppose someone asked you to devise the most powerful computer possible. Alan Turing, whose reputation as a central figure in computer science and artificial intelligence has only grown since his untimely death in 1954, applied his genius to problems such as this one in an age before computers as we know them existed. His theoretical work on this problem and others remains a foundation of computing, AI and modern cryptographic standards, including those NIST recommends.

The road from devising the most powerful computer possible to cryptographic standards has a few twists and turns, as does Turing's brief life.

In Turing's time, mathematicians debated whether it was possible to build a single, all-purpose machine that could solve all problems that are computable. For example, we can compute a car's most energy-efficient route to a destination, and (in principle) the most likely way in which a string of amino acids will fold into a three-dimensional protein. Another example of a computable problem, important to modern encryption, is whether or not bigger numbers can be expressed as the product of two smaller numbers. For example, 6 can be expressed as the product of 2 and 3, but 7 cannot be factored into smaller integers and is therefore a prime number.

Some prominent mathematicians proposed elaborate designs for universal computers that would operate by following very complicated mathematical rules. It seemed overwhelmingly difficult to build such machines. It took the genius of Turing to show that a very simple machine could in fact compute all that is computable.

His hypothetical device is now known as a “Turing machine.” The centerpiece of the machine is a strip of tape, divided into individual boxes. Each box contains a symbol (such as A,C,T, G for the letters of genetic code) or a blank space. The strip of tape is analogous to today’s hard drives that store bits of data. Initially, the string of symbols on the tape corresponds to the input, containing the data for the problem to be solved. The string also serves as the memory of the computer. The Turing machine writes onto the tape data that it needs to access later in the computation.



The device reads an individual symbol on the tape and follows instructions on whether to change the symbol or leave it alone before moving to another symbol. The instructions depend on the current “state” of the machine. For example, if the machine needs to decide whether the tape contains the text string “TC” it can scan the tape in the forward direction while switching among the states “previous letter was T” and “previous letter was not C.” If while in state “previous letter was T” it reads a “C,” it goes to a state “found it” and halts. If it encounters the blank symbol at the end of the input, it goes to the state “did not find it” and halts. Nowadays we would recognize the set of instructions as the machine’s program.

It took some time, but eventually it became clear to everyone that Turing was right: The Turing machine could indeed compute all that seemed computable. No number of additions or extensions to this machine could extend its computing capability.

To understand what can be computed it is helpful to identify what cannot be computed. In a previous life as a university professor I had to teach programming a few times. Students often encounter the following problem: “My program has been running for a long time; is it stuck?” This is called the Halting Problem, and students often wondered why we simply couldn’t detect infinite loops without actually getting stuck in them. It turns out a program to do this is an impossibility. Turing showed that there does not exist a machine that detects whether or not another machine halts. From this seminal result followed many other impossibility results. For example, logicians and philosophers had to abandon the dream of an automated way of detecting whether an assertion (such as whether there are infinitely many prime numbers) is true or false, as that is uncomputable. If you could do this, then you could solve the Halting Problem simply by asking whether the statement “this machine halts” is true or false.

Turing went on to make fundamental contributions to AI, theoretical biology and cryptography. His involvement with this last subject brought him honor and fame during World War II, when he played a very important role in adapting and extending cryptanalytic techniques invented by Polish mathematicians. This work broke the German Enigma machine encryption, making a significant contribution to the war effort.

Turing was gay. After the war, in 1952, the British government convicted him for having sex with a man. He stayed out of jail only by submitting to what is now called "chemical castration." He died in 1954 at age 41 by cyanide poisoning, which was initially ruled a suicide but may have been an accident according to subsequent analysis. More than 50 years would pass before the British government apologized and "pardoned" him (after years of campaigning by scientists around the world). Today, the highest honor in computer sciences is called the Turing Award.

Turing's computability work provided the foundation for modern complexity theory. This theory tries to answer the question "Among those problems that can be solved by a computer, which ones can be solved efficiently?" Here, "efficiently" means not in billions of years but in milliseconds, seconds, hours or days, depending on the computational problem.

For example, much of the cryptography that currently safeguards our data and communications relies on the belief that certain problems, such as decomposing an integer number into its prime factors, cannot be solved before the Sun turns into a red giant and consumes the Earth (currently forecast for 4 billion to 5 billion years). NIST is responsible for cryptographic standards that are used throughout the world. We could not do this work without complexity theory.

Technology sometimes throws us a curve, such as the discovery that if a sufficiently big and reliable quantum computer is built it would be able to factor integers, thus breaking some of our cryptography. In this situation, NIST scientists must rely on the world's experts (many of them in-house) in order to update our standards. There are deep reasons to believe that quantum computers will not be able to break the cryptography that NIST is about to roll out. Among these reasons is that Turing's machine can simulate quantum computers. This implies that complexity theory gives us limits on what a powerful quantum computer can do.

But that is a topic for another day. For now, we can celebrate how Turing provided the keys to much of today's computing technology and even gave us hints on how to solve looming technological problems.

15. EY Survey: Most UK Business Leaders Expect Quantum Computing Disruption, But Planning Lags

by Matt Swayne

https://thequantuminsider.com/2022/06/24/ey-survey-most-uk-business-leaders-expect-quantum-computing-disruption-but-planning-lags/?utm_source=newsletter&utm_medium=email&utm_term=2022-06-25&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Sensing+Interest+in+Sensors+Hubs+and+Networks+--+And+More+Quantum+News

EY's Quantum Readiness Survey 2022, produced in collaboration with the National Quantum Computing Centre (NQCC), has found that 81% of senior UK executives expect quantum computing to play a significant role in their industry by 2030.

This research marks a continuation of the UK's commitment to developing its quantum computing capabilities, spearheaded by the NQCC alongside policy makers, academia and industry. The NQCC represents a £93m UK Government investment over five years through UK Research and Innovation (UKRI) with the aim of placing the UK at the cutting edge of quantum computing.

Despite growing anticipation among senior leaders, strategic planning for quantum computing is in early stages for most organisations. For example, only 33% are engaged in strategic planning related to quantum computing and a quarter have appointed specialist leaders or set up pilot teams.

Quantum computing is in its relative infancy as a technology, but its transformative potential is already being recognised by the UK's business leaders. While the majority believe its full impact will not be felt immediately, almost half (48%) think that quantum will begin to transform industries as soon as 2025.

Furthermore, respondents were almost unanimous in their belief that quantum computing will create a moderate or high level of disruption of their own organisation, industry sector, and the broader UK economy in the next five years.

Different sectors of the economy have differing views on the timeline for quantum computing's maturation. Executives in consumer products and retail are most optimistic, with 70% believing quantum will play a significant role by 2025.

Meanwhile, 56% of telecoms, media and entertainment, and technology (TMT) executives foresee the same impact in this timeframe. However, most respondents in health and life sciences companies think maturation is more likely to occur between 2026 and 2035.

Science Minister George Freeman said: "The UK is at the forefront of a quantum computing revolution that will deliver exponential increases in computer processing power, opening up the possibility to solve problems that were previously unachievable.

"I am pleased to see from this report that business leaders across our economy recognise just how transformational quantum technology will be for the future of their industries, and the work that still needs to be done to get this technology where it needs to be.

"This is why I have made it a priority for this government to develop our National Quantum Strategy this year – to set out a clear plan for ensuring the UK's leadership in quantum applications that will be able to support industries from life sciences to finance."

Planning for quantum is lagging behind

Despite the majority of survey respondents forecasting quantum disruption by 2030 or sooner, strategic planning cycles for quantum are lagging behind. Most organisations expect to start their quantum journeys in the next one to two years. Almost three-quarters (72%) will start planning by 2024.

This will involve recruiting people to lead quantum computing efforts across the organisation. Only 25% of the organisations surveyed have done this, but 71% are hopeful of appointing a specialist quantum head in the next two years.

As well as hiring leaders, respondents are aiming to set up pilot teams to explore the potential of quantum for their business: over two-thirds (68%) expect to have done this by 2024, but only 24% have done so already.

Piers Clinton-Tarestad, Quantum Computing Leader EY UKI said: "This study reveals a disconnect between the pace at which industry leaders expect quantum to start significantly transforming businesses and their general preparedness for its impact. Maximising the potential of quantum technologies will require early planning to build responsive and adaptable organisational capabilities – which is a challenge because while the progress of quantum has accelerated it is not following a steady trajectory.

"Quantum readiness" is not so much a gap to be assessed as a road to be walked, with next steps being regularly revisited as the landscape evolves. Businesses that expect industry disruption within the next three or five years, therefore, need to act now."

Competitive advantage and hi-tech use-cases driving quantum optimism

As with any nascent technology, the drivers for investing in quantum computing are varied and in development.

One factor playing on the minds of almost half (47%) of business leaders is that rival firms are working to develop their own quantum capabilities, which may possibly give them a competitive advantage. Almost all respondents (97%) believe that their competitors are currently engaging with quantum computing in some capacity.

In terms of use-cases, the most promising application for quantum computing foreseen by industry leaders is enhancing operations involving AI and machine learning. This was especially true of leaders within financial services, automotive and manufacturing.

Quantum's ability to accelerate computational modelling and simulations are front of mind for those in health and life sciences, while TMT respondents cited its potential to evolve existing methods of cryptography and encryption as its most critical function.

Dr Simon Plant, Deputy Director for Innovation, National Quantum Computing Centre said: "Quantum computing is expected to significantly speed up the time to solution for certain tasks, addressing computational problems that are currently intractable using conventional digital technologies. The pace of development is accelerating, and the question is how and when – not if – quantum computing can address industrially-relevant use cases. There is a perceived first-mover advantage in being prepared to harness the capabilities as they emerge and build resilience into forward plans."

The NQCC is working with businesses, government and the research community to deliver quantum computing capabilities for the UK and support the growth of the emerging industry. This report is a key part of that work helping explain why the UK needs to be at the forefront of quantum computing and to demonstrate how strategically important this technology is to the country.

16.Linking two independent quantum nodes for future metropolitan quantum networks

https://qutech.nl/2022/06/22/linking-nodes-for-metropolitan-networks/

Researchers at QuTech have demonstrated a key technology for linking quantum nodes over existing telecom fiber, by realizing quantum interference of photons emitted by quantum devices at telecom wavelengths. The technique also allows for compensating intrinsic differences between the quantum devices. The work is published in PRX Quantum and is an important step for bringing quantum networks out of the lab and into real-world settings.

Quantum networks hold the promise of fundamentally changing the way we share and process information. A future quantum internet, built using quantum processor nodes connected via optical channels, will enable applications ranging from secure communication to cloud computing with full privacy and enhanced sensing.

Entanglement between network nodes

For a quantum network to function it uses a particular quantum effect between the nodes in the network called quantum entanglement. Practically entanglement means that the state of a second qubit (that can be '1' or 'up') is dictated by the state of a first qubit (i.e. '0' or 'down'). This entanglement can be used for generating secret keys for private communication, or teleportation of a quantum state between far away parties. QuTech was the first to establish a multi-node network in the lab [link], by using optically active spins in solids.

Entanglement between network nodes is generated by first entangling the spins with flying photonic qubits and then interfering those photons in a connecting middle station. For scaling this approach to larger networks two major challenges arise. "Leading platforms for a future quantum network emit photons in the visible spectrum and fiber losses at these frequencies hinder scaling beyond a few kilometers", says first author Arian Stolk. "So, to bring these quantum networks out of the lab and to move towards metropolitan scale, it is crucial to convert the frequencies of the photons to the telecom band, whilst maintaining their quantum feature. Moreover, overcoming the intrinsic variations between our quantum chips and ensuring compatibility with other nodes is a challenge for scaling up. In this paper, we introduce a method that tackles both these challenges simultaneously."

Solving fiber loss and variations between chips

The approach used to tackle the challenges is based on a technique called 'quantum frequency conversion'. It uses a strong pump laser that interacts with the single photons inside a specially designed crystal, subtracting energy in the process. The exact frequency that the single photons end up with can be controlled by adjusting the pump laser frequency, giving the researcher the ability to precisely match different nodes over a network.

From visible wavelengths in the lab to telecom bands

The researchers at QuTech—a collaboration between TNO and TU Delft—demonstrate their technique by building two remote quantum nodes based on the nitrogen-vacancy (NV) center in diamond. "We show that the resonant emission of the NV centers (around 637nm) can be faithfully converted very precisely to a wavelength in the telecom L-band (1588nm) by locking to a central reference laser, over a broad range of frequencies. This technique facilitates scaling by removing the difference in emission frequency between nodes that existed before the conversion."

The way the researchers verified their scheme is through an interference experiment. It is done by sending single photons from the remote nodes through their respective converters, towards a beam splitter, after which they are detected. For the photons that were expected to be indistinguishable from each other, a reduction in simultaneous clicks in the detectors was observed, in line with the theory describing the process. "Further analysis finds a high degree of indistinguishability of the converted photons, emphasizing the effectiveness of our scheme", says Stolk.

Towards 20 km deployment

Looking forward, the presented results are an important milestone towards achieving entanglement of NV center nodes over tens of kilometers of deployed telecom fibers. Great effort has already been taken to prepare the nodes for operation over such a long-range connection. Entanglement between solid state quantum processors over such distance would constitute a proof of principle for future entanglement-based quantum networks on a metropolitan/national scale. "We also believe that other quantum platforms in diamond, silicon, and silicon carbide that emit in the visible spectrum, can benefit from our technique."

17.The Next Generation of IBM Quantum Computers

by Kevin Krewell

https://www.forbes.com/sites/tiriasresearch/2022/06/22/the-next-generation-of-ibm-quantum-computers/?sh=177736266f57

In my previous article on IBM Quantum computers, I wrote about IBM's plans to improve access to its quantum computers. This article describes the update to IBM's Quantum computing roadmap as revealed by Darío Gil, Senior Vice President, Director of Research at IBM Think in June.

IBM is building accessible, scalable quantum computing by focusing on three pillars:

- Increasing qubit counts
- Developing advanced quantum software that can abstract away infrastructure complexity and orchestrate quantum programs
- Growing an ecosystem of quantum-ready enterprises, organizations, and communities

IBM originally announced its quantum development roadmap in 2020. To date, the company has hit its planned releases on the original timeline. In addition to new quantum systems, IBM has sped execution performance by 120x using Qiskit Runtime, IBM's containerized quantum computing service and programming model, from previous experiments.

The next step in IBM's goals to build a frictionless development experience will be the release of Qiskit Runtime in 2022, which will allow developers to build workflows in the cloud, offering greater flexibility. Bringing a serverless approach to quantum computing will also provide the flexibility to distribute workloads intelligently and efficiently across quantum and classical systems.

To help speed the work of developers, IBM launched Qiskit Runtime primitives earlier this year. The primitives implement common quantum hardware queries used by algorithms to simplify quantum programming. In 2023, IBM plans to expand these primitives, as well as the capability to run on the next generation of parallelized quantum processors.

Quantum Hardware Scaling

Later this year, IBM is scheduled to deliver the 433-qubit Osprey quantum computer and dynamic circuits. IBM used 3D packaging to place a complex tangle of microwave circuit components and wiring on multiple physical levels close to the quantum processors, enabling the faster execution of dynamic quantum circuits. IBM's experience packaging qubits will then enable construction of the 1121-qubit Condor computer, with minimal impact to individual qubit performance, in 2023. IBM expects Condor to be the first quantum computer with more than 1,000 qubits. After Condor, IBM will use chip-to-chip couplers to build even larger quantum systems.

"Our new quantum roadmap shows how we intend to achieve the scale, quality, and speed of computing necessary to unlock the promise of quantum technology," said Jay Gambetta, VP of Quantum Computing and IBM Fellow. "By combining modular quantum processors with classical infrastructure, orchestrated by Qiskit Runtime, we are building a platform that will let users easily build quantum calculations into their workflows and so tackle the essential challenges of our time."

To build this new quantum roadmap, IBM is targeting three scalability "regimes" or steps to scale its quantum processors.

The first step requires building capabilities to "classically" communicate and parallelize operations in a non-quantum way across multiple processors. This step opens the door to a broader set of techniques such as improved error mitigation techniques and intelligent workload orchestration, which combine classical compute capabilities with quantum processors.

The next step is building short-range, chip-level couplers between quantum chips. Using these couplers, multiple chips can be connected to effectively form a single larger processor. This multichip modularity is key to scaling.

Ultimately, the third step to reach larger scalability is developing quantum communication links between quantum processors. These quantum communication links connect clusters of quantum processors together into a larger quantum system.

IBM plans to be using all three of these scalability techniques by 2025 to build a 4,000+ qubit processor based on multiple clusters of modularly scaled processors.

Future quantum computing systems will be called **IBM Quantum System Two**. A central approach to building IBM Quantum System Two will be modularity, which will be necessary to increase the scale of IBM quantum chips in the future.

System Two introduces a new generation of scalable qubit control electronics together with higher-density cryogenic components and cabling. The platform brings the possibility of providing a larger shared cryogenic workspace, opening the door to potential linking of quantum processors through novel interconnects. System Two is a major step toward a true quantum data center. A prototype of this system is targeted to be up and running in 2023.

While building systems with more qubits is important for extending the capabilities of quantum computing, the quality of these qubits is also essential to building practical quantum computers. Qubit quality refers to the amount of time that the qubits are entangled and the error rate of the results. IBM has a metric for qubits called Quantum Volume (QV). IBM says its quantum systems are moving from a QV of 256 last year, to a QV of 1024 this year. The Falcon r10 system has under a 1 in 1000 error rate today. IBM handles its error management in the Quiskit Runtime.

There is progress being made with error mitigation and suppression techniques to improve the ability of quantum software to minimize the effect of noise on the users' application. These are important steps on the path towards the error-corrected quantum systems of the future.

Multichip connectivity

The next step to scaling quantum computers will be to make quantum communications links between chips and between cryostats. First, IBM plans to connect three or more Heron 133 qubit chips using classical (non-quantum) logic connections in 2023. With classical interconnects, the quantum state must be resolved to a binary logical result. But with the Crossbill quantum computer in 2024, IBM plans to interconnect chips with quantum entangled connections, which communicate in a quantum state. The connection between three chips should deliver 408 qubits. IBM will offer both system scaling options for experiments.

In addition to the potential for using quantum computing to solve complex problems, this technology can also be used to crack today's data encryption. While some cryptographers are skeptical that quantum computing can reliably be used to break cryptography within the next decade, IBM is already planning to mitigate the issue by offering quantum-safe cryptography. For example, the recently announced Telum Z16 mainframe has quantum-safe encryption.

Summary

IBM continues to leverage its traditional computing, quantum expertise, packaging technology, extensive software resources, and new business models to expand the developer reach and market opportunities for quantum computers. IBM's super-cold qubits are also fast — 1,000 times faster than Ion-trap quantum computers. The company has committed to scaling quantum computing and adding greater capabilities over a multi-year roadmap.

18.Cryptography safe for now, but urgent need to build quantum skills

by Eileen Yu
https://www.zdnet.com/article/cryptography-safe-for-now-but-urgent-need-to-build-quantum-skills/

It is premature to sound the death knell for current key cryptography, but there is an urgent need now to build up skillsets in quantum computing. This will ensure nations have the right knowledge to combat potential threats when the technology becomes viable in the near future.

And that future may play out in the next five years as market players make significant strides in the field. IBM, for instance, said it planned to produce a quantum computer capable of clocking at least 4,000 qubits by 2025. This would push the technology past experimental stage, with organisations able to deploy quantum computers within the 2023 to 2025 timeframe, IBM said.

Such progress underscored the need to ensure there were skillsets ready to tap and support future deployment of quantum computing, said Dell Technologies CTO John Roese.

Noting that the tech community was ill-prepared for the emergence of cloud computing, he said there were professionals skilled in traditional programming languages such as C++, but there was a dearth of relevant skillsets to leverage cloud-native architectures.

Businesses and universities realised this and made the effort to catch up, Reese said in an interview with ZDNet.

While the industry managed to scrape through, he urged the need to learn from this mistake and prepare for the next shift. This would ensure governments and organisations were ready when quantum computers were commercially available.

He said the technology field required a different set of skills as the programming language and build logic were different. Software frameworks and tool chains also were new, so the tech workforce including data scientists would have to adapt and build up new skillsets for quantum computing.

Efforts here at least appear to be underway. Dell estimates that governments worldwide have committed upwards of $24 billion in research and development investments to establish competencies around quantum technology.

This was significant, Roese said, considering the industry today was worth just $900 million in revenue. He added that Asian nations such as China, Singapore, and India were amongst those that had begun work to build up capabilities in quantum computing.

In Singapore, such plans included focus on security and building quantum-safe networks. The government last month announced it was setting aside SG$23.5 million (17.09 million) to support three national platforms, parked under its Quantum Engineering Programme (QEP), for up to 3.5 years.

These aimed to boost the country's capabilities in quantum computing and ensure encryption technologies remained robust and able to withstand "brute force" attacks.

The QEP also encompassed a quantum-safe network touted to showcase "crypto-agile connectivity" and support trials with both public and private organisations. First unveiled in February, the project aimed to enhance network security for critical infrastructures and had roped in 15 partners at launch, including ST Telemedia Global Data Centres, Cyber Security Agency, and Amazon Web Services.

Singapore's Deputy Prime Minister and Coordinating Minister for Economic Policies Heng Swee Keat said quantum technology could prove a "game changer", as efforts were made to stay ahead of malicious actors amidst a cyber landscape that was fast evolving.

Heng said: "Strong encryption is key to the security of digital networks. The current encryption standard, AES 256, has held up, as few have the computing power to use brute force to break the encryption. But this could change with quantum computing."

As quantum computers continued to achieve higher compute speeds million times faster than supercomputers, he said it was vital that Singapore invested in quantum engineering and research to stay ahead of potential threats.;

Roese noted that while public key cryptography remained robust today, the threat quantum advancements presented was "real enough" and could pose certain risks in the future.

Personal medical information and certain banking data, in particular, that were permanent records and would remain relevant 10 years down the road must stay secured against future threats.

"So the risk isn't about exposing the information now, but whether it is potentially vulnerable 10 years from now," he said, adding that governments also would want to ensure communications between nation states remained secured decades on, as a breach could lead to a sticky geopolitical situation.

He pointed to the need for tools to support crypto "agility", which would allow organisation to decide what kind of data should be wrapped in post-quantum encryption.

Asked where Dell fit in the quantum space, Roese said the tech vendor was not looking to produce quantum computers. Instead, it aimed to provide the tools and capabilities to piece together what was required to make such systems viable.

Describing the end state for quantum computers as the "quantum sandwich", he said Dell was working with key quantum players including IBM to determine the best way to architect and pull in conventional computer architectures, such as servers, so these could operate efficiently with quantum at the core.

Part of Dell's efforts here encompassed a hybrid emulation platform that could enable developers to run quantum applications on classical computing infrastructure.

Roese said: "There are very few quantum computers being built today. To put one into production doesn't involve just the quantum component, but the surrounding parts and you then need to operationalise it."

Dell hoped to drive this by "industrialising" the innovation and making it useable, he said, adding that it aimed to do so through its quantum simulation platform and hybrid quantum architecture systems.

19.AWS Opens Center for Quantum Networking

by Matt Swayne

https://thequantuminsider.com/2022/06/21/aws-opens-center-for-quantum-networking/?utm_source=newsletter&utm_medium=email&utm_term=2022-06-25&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Sensing+Interest+in+Sensors+Hubs+and+Networks+--

+And+More+Quantum+News

Work on quantum at AWS reaches across timescales — from investigating quantum technologies for near-term impact to developing the tools and technology that will, on the long-term, lead to robust quantum computing.

AWS, a subsidiary of Amazon, announced the creation of the AWS Center for Quantum Networking, which will focus on solving some of those long-term challenges associated the quantum industry is facing.

"Today we announce the AWS Center for Quantum Networking (CQN) with a mission to address these fundamental scientific and engineering challenges and to develop new hardware, software and applications for quantum networks," the company announced in a blog post. "CQN will complement the advanced quantum science and engineering efforts already underway at AWS Center for Quantum Computing and Amazon Quantum Solutions Lab."

According to the post, investment in the long-term has already had an impact on quantum computing right now.

They write: "While there is still a long way ahead, these investments have already transformed quantum computers: They have evolved from delicate laboratory systems accessible to only a few research institutions to increasingly reliable and powerful commercial machines available to researchers, developers, and even quantum enthusiasts worldwide via cloud services like Amazon Braket."

Quantum's progress is being backed by investments from governments and technology companies, such as AWS.

As investments in quantum grow, AWS sees a need for quantum networks to fulfill the true potential of quantum devices. These networks are similar to the backbone of today's internet — but much more powerful and with far more interesting features.

"Despite not receiving the same level of attention as quantum computers, quantum networks have fascinating possible applications," they write. "One of them is enabling global communications protected by quantum key distribution with privacy and security levels not achievable using conventional encryption techniques. Quantum networks will also provide powerful and secure cloud quantum servers by connecting together and amplifying the capabilities of individual quantum processors."

Some technologies that will be used in quantum networks are already available, including lasers, fibers, and detectors. However, quantum networks require single photons — smallest building blocks of light — to connect quantum devices together, rather than instead of strong laser beams. While single photons will make quantum networks work, they also pose challenges. They can not be amplified, which limits the network range. And, according to the post, single photons are weak, which makes them difficult to interface with quantum computing devices.

Entirely new technologies — such as quantum repeaters and transducers — will need to be developed to make global quantum networks.

“Like quantum computers, quantum networks are still at an early stage of development, with many outstanding challenges remaining before their full potential is reached,” they write. “Through our investment in quantum research and workforce development, the AWS CQN aims to bring quantum network-enabled advances in privacy, security, and computational power one step closer to our customers.”

20.`Hertzbleed’ Side-Channel Attack Threatens Cryptographic Keys for Servers

by Tara Seals

https://www.darkreading.com/attacks-breaches/hertzbleed-side-channel-attack-cryptographic-keys-servers

A side-channel timing attack dubbed "Hertzbleed" by researchers could allow remote attackers to sniff out cryptographic keys for servers. It affects most Intel processors, as well as some chipsets from AMD and likely others.

The issue is a timing side-channel flaw (tracked as CVE-2022-24436 for Intel and CVE-2022-23823 for AMD) found in the CPU-throttling technology known as dynamic voltage and frequency scaling (DVFS). DVFS regulates power consumption and electrical current use so that a CPU doesn't overheat when processing large amounts of data, and it conserves battery power during low-activity times.

As Intel explains in guidance published this week, observing these regulation changes can allow attackers to infer sensitive information.

"CPU frequency throttling is triggered when one of these limits is reached, which results in CPU frequency," according to Intel. "This frequency change and derived behavior may be correlated with information being processed by the CPU, and it may be possible to infer parts of the information through sophisticated analysis of the frequency change behavior." "In the worst case, these attacks can allow an attacker to extract cryptographic keys from remote servers that were previously believed to be secure," according to a technical research paper (PDF) by the team who discovered the attack, from the University of Texas at Austin, the University of Illinois Urbana-Champaign, and the University of Washington.

Hertzbleed – its name a take on the infamous "Heartbleed" timing attack from 2014 – is significant because it allows remote attacks without the need to subvert a power-measurement interface, the researchers note, thus widening the attack surface.

"Software-based power-analysis attacks can be mitigated and easily detected by blocking (or restricting [10]) access to power-measurement interfaces," according to the paper. "Up until today, such a mitigation strategy would effectively reduce the attack surface to physical power analysis, a significantly smaller threat."

Actual Threat or Not?

While the researchers acknowledge that any real-world attacks would require a high level of complexity, they demonstrated successful proofs of concept for extracting keys as remote attackers authenticated with low privileges and no user interaction requires. This makes "Hertzbleed is a real, and practical, threat to the security of cryptographic software," they say.

Intel begs to differ.

"While this issue is interesting from a research perspective, we do not believe this attack to be practical outside of a lab environment," said Jerry Bryant, Intel's senior director of security communications and incident response, in a recent posting. "Also note that cryptographic implementations that are hardened against power side-channel attacks are not vulnerable to this issue."

However, he also explained that the issue may extend past Intel and AMD.

"CVE-2022-24436 is not architecture-specific and any modern CPU that has dynamic power and thermal management is potentially affected," he said. "Intel shared its findings with other silicon vendors so they could assess their potential impact."

Neither Intel nor AMD are issuing microcode to address the issue; instead, they recommend that developers achieve mitigation through masking and blinding techniques that would hide the timing changes from observation.

21.What quantum information and snowflakes have in common, and what we can do about it

by Daniel Strain
https://www.colorado.edu/today/2022/06/15/how-handle-quantum-information-without-destroying-it

Qubits are a basic building block for quantum computers, but they're also notoriously fragile—tricky to observe without erasing their information in the process. Now, new research from CU Boulder and the National Institute of Standards and Technology (NIST) may be a leap forward for handling qubits with a light touch.

In the study, a team of physicists demonstrated that it could read out the signals from a type of qubit called a superconducting qubit using laser light—and without destroying the qubit at the same time.

The group's results could be a major step toward building a quantum internet, the researchers say. Such a network would link up dozens or even hundreds of quantum chips, allowing engineers to solve problems that are beyond the reach of even the fastest supercomputers around today. They could also, theoretically, use a similar set of tools to send unbreakable codes over long distances.

The study, published June 15 in the journal Nature, was led by JILA, a joint research institute between CU Boulder and NIST.

"Currently, there's no way to send quantum signals between distant superconducting processors like we send signals between two classical computers," said Robert Delaney, lead author of the study and a former graduate student at JILA.

Quantum computers, which run on qubits, get their power by tapping into the properties of quantum physics, or the physics governing very small things. Delaney explained the traditional bits that run your laptop are pretty limited: They can only take on a value of zero or one, the numbers that underly most computer programming to date. Qubits, in contrast, can be zeros, ones or, through a property called "superposition," exist as zeros and ones at the same time.

But working with qubits is also a bit like trying to catch a snowflake in your warm hand. Even the tiniest disturbance can collapse that superposition, causing them to look like normal bits.

In the new study, Delaney and his colleagues showed they could get around that fragility. The team uses a wafer-thin piece of silicon and nitrogen to transform the signal coming out of a superconducting qubit into visible light—the same sort of light that already carries digital signals from city to city through fiberoptic cables.

"Researchers have done experiments to extract optical light from a qubit, but not disrupting the qubit in the process is a challenge," said study co-author Cindy Regal, JILA fellow and associate professor of physics at CU Boulder.

Fragile qubits

There are a lot of different ways to make a qubit, she added.

Some scientists have assembled qubits by trapping an atom in laser light. Others have experimented with embedding qubits into diamonds and other crystals. Companies like IBM and Google have begun designing quantum computer chips using qubits made from superconductors.

Superconductors are materials that electrons can speed around without resistance. Under the right circumstances, superconductors will emit quantum signals in the form of tiny particles of light, or "photons," that oscillate at microwave frequencies.

And that's where the problem starts, Delaney said.

To send those kinds of quantum signals over long distances, researchers would first need to convert microwave photons into visible light, or optical, photons—which can whiz in relative safety through networks fiberoptic cables across town or even between cities. But when it comes to quantum computers, achieving that transformation is tricky, said study co-author Konrad Lehnert.

In part, that's because one of the main tools you need to turn microwave photons into optical photons is laser light, and lasers are the nemesis of superconducting qubits. If even one stray photon from a laser beam hits your qubit, it will erase completely.

"The fragility of qubits and the essential incompatibility between superconductors and laser light makes usually prevents this kind of readout," said Lehnert, a NIST and JILA fellow.

Secret codes

To get around that obstacle, the team turned to a go-between: a thin piece of material called an electro-optic transducer.

Delaney explained the team begins by zapping that wafer, which is too small to see without a microscope, with laser light. When microwave photons from a qubit bump into the device, it wobbles and spits out more photons—but these ones now oscillate at a completely different frequency. Microwave light goes in, and visible light comes out

In the latest study, the researchers tested their transducer using a real superconducting qubit. They discovered the thin material could achieve this switcheroo while also effectively keeping those mortal enemies, qubits and lasers, isolated from each other. In other words, none of the photons from the laser light leaked back to disrupt the superconductor.

"Our electro-optic transducer does not have much effect on the qubit," Delaney said.

The team hasn't gotten to the point where it can transmit actual quantum information through its microscopic telephone booth. Among other issues, the device isn't particularly efficient yet. It takes about 500 microwave photons, on average, to produce a single visible light photon.

The researchers are currently working to improve that rate. Once they do, new possibilities may emerge in the quantum realm. Scientists could, theoretically, use a similar set of tools to send quantum signals over cables that would automatically erase their information when someone was trying to listen in. Mission Impossible made real, in other words, and all thanks to the sensitive qubit.

22.What China's targeting of US telecoms means for post-quantum security

by Zhanna L. Malekos Smith

https://thehill.com/opinion/cybersecurity/3520574-what-chinas-targeting-of-us-telecoms-means-for-post-quantum-security/

Ceding the initiative to an adversary is a difficult position to recover from — even in cyberspace. Chinese state-sponsored cyber actors are seizing the initiative to exploit publicly known vulnerabilities to unpatched network devices, such as home office routers, to compromise major U.S. telecommunications companies and network service providers, the FBI and other agencies warn in the latest joint cybersecurity advisory.

These cyber actors are infiltrating victims' accounts by "using publicly available exploit code against virtual private network (VPN) services, or public facing applications — without using their own distinctive or identifying malware — so long as the actors acted before victim organizations updated their systems," the advisory explained.

While defending against common vulnerabilities is essential, the Biden administration must maintain the initiative against post-quantum cryptography threats. Post-quantum refers to the stage when quantum computers advance to "a sufficient size and level of sophistication" that they break the cryptography that secures our digital communications and financial transactions on the internet. These systems are cryptanalytically relevant quantum computers, meaning they could pose significant national, economic and cybersecurity risks to the United States by weakening the public-key cryptography we rely on to communicate.

It is not a question of if, but when cryptanalytically relevant quantum computers will be developed, according to the White House's fact sheet on quantum technologies, which estimates this milestone is attainable "at some point in the not-too-distant future."

Last May, the Biden administration enacted two directives to expand the 2018 National Quantum Initiative Act: an executive order establishing a committee to advise the White House about the National Quantum Initiative program; and the National Security Memorandum on Promoting United States Leadership in Quantum Computing. The memorandum warns that quantum information science presents significant security risks to cryptographic systems that safeguard critical infrastructure and secure military and civilian communications.

The White House cautioned that this class of computers could "jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions." Just as there is an eagerness to reap the scientific and commercial benefits of quantum information sciences and technology — a broad discipline of science and engineering — there is an equal sense of apprehension about the accompanying risks that "quantum supremacy" could bring to national and economic security. Quantum supremacy refers to a technological milestone when the computational speed and power of quantum computers could outperform that of classical computers.

Although the practical applications of quantum computing aren't here yet, the technology holds tremendous potential for advancing the United States' economy and supporting research in bioengineering, artificial intelligence and machine learning, and even financial market analysis.

Some companies are forming international quantum research partnerships to accelerate growth in the global market. In 2021, IBM helped Germany become the first European country to develop a quantum computer and plans to build quantum systems in Canada and South Korea by 2023. While commercial opportunities for collaboration abound, there is also an intensifying political competition amongst states to gain a competitive edge.

China, Russia and the United States are competing to become the leader in advanced computing before 2030. Other countries also are prioritizing quantum information sciences — France aspires to be one of the world's leaders in quantum and supports the European Union's Digital Compass project to produce its first domestic quantum computer by 2025. The United Kingdom is steadily investing in the National Quantum Computing Centre, following Prime Minister Boris Johnson's call to "go big on quantum computing." Japan's government announced it will establish four quantum research centers and produce its first domestic quantum computer by March 2023.

The White House memorandum forewarns of "future attacks" against U.S. information technology infrastructure and emphasizes the need to begin updating systems to better protect against a post-quantum risk environment. Acknowledging these risks, it champions setting requirements for federal agencies to transition vulnerable cryptographic systems to using quantum-resistant cryptographic standards.

Preparation is a quintessential element of success. Transitioning infrastructure toward federally approved standards is not a small undertaking; iterative reviews will require discipline and patience. Thankfully, the National Institute of Standards and Technology is working with stakeholders in its call for proposals to produce quantum-resistant cryptographic standards by 2024.

By concentrating national resources on this complex challenge now, the United States will be better positioned to operate and thrive in a post-quantum environment.

23.A new vulnerability in Intel and AMD CPUs lets hackers steal encryption keys

by Dan Goodin

https://arstechnica.com/information-technology/2022/06/researchers-exploit-new-intel-and-amd-cpu-flaw-to-steal-encryption-keys/

Microprocessors from Intel, AMD, and other companies contain a newly discovered weakness that remote attackers can exploit to obtain cryptographic keys and other secret data traveling through the hardware, researchers said on Tuesday.

Hardware manufacturers have long known that hackers can extract secret cryptographic data from a chip by measuring the power it consumes while processing those values. Fortunately, the means for exploiting power-analysis attacks against microprocessors is limited because the threat actor has few viable ways to remotely measure power consumption while processing the secret material. Now, a team of researchers has figured out how to turn power-analysis attacks into a different class of side-channel exploit that's considerably less demanding.

Targeting DVFS

The team discovered that dynamic voltage and frequency scaling (DVFS)—a power and thermal management feature added to every modern CPU—allows attackers to deduce the changes in power consumption by monitoring the time it takes for a server to respond to specific carefully made queries. The discovery greatly reduces what's required. With an understanding of how the DVFS feature works, power side-channel attacks become much simpler timing attacks that can be done remotely.

The researchers have dubbed their attack Hertzbleed because it uses the insights into DVFS to expose—or bleed out—data that's expected to remain private. The vulnerability is tracked as CVE-2022-24436 for Intel chips and CVE-2022-23823 for AMD CPUs. The researchers have already shown how the exploit technique they developed can be used to extract an encryption key from a server running SIKE, a cryptographic algorithm used to establish a secret key between two parties over an otherwise insecure communications channel.

The researchers said they successfully reproduced their attack on Intel CPUs from the 8th to the 11th generation of the Core microarchitecture. They also claimed that the technique would work on Intel Xeon CPUs and verified that AMD Ryzen processors are vulnerable and enabled the same SIKE attack used against Intel chips. The researchers believe chips from other manufacturers may also be affected.

In a blog post explaining the finding, research team members wrote:

> Hertzbleed is a new family of side-channel attacks: frequency side channels. In the worst case, these attacks can allow an attacker to extract cryptographic keys from remote servers that were previously believed to be secure.
>
> Hertzbleed takes advantage of our experiments showing that, under certain circumstances, the dynamic frequency scaling of modern x86 processors depends on the data being processed. This means that, on modern processors, the same program can run at a different CPU frequency (and therefore take a different wall time) when computing, for example, `2022 + 23823` compared to `2022 + 24436`.

Hertzbleed is a real, and practical, threat to the security of cryptographic software.
We have demonstrated how a clever attacker can use a novel chosen-ciphertext attack against SIKE to perform full key extraction via remote timing, despite SIKE being implemented as "constant time".

Intel Senior Director of Security Communications and Incident Response Jerry Bryant, meanwhile, challenged the practicality of the technique. In a post, he wrote: "While this issue is interesting from a research perspective, we do not believe this attack to be practical outside of a lab environment. Also note that cryptographic implementations that are hardened against power side-channel attacks are not vulnerable to this issue." Intel has also released guidance here for hardware and software makers.

Neither Intel nor AMD are issuing microcode updates to change the behavior of the chips. Instead, they're endorsing changes Microsoft and Cloudflare made respectively to their PQCrypto-SIDH and CIRCL cryptographic code libraries. The researchers estimated that the mitigation adds a decapsulation performance overhead of 5 percent for CIRCL and 11 percent for PQCrypto-SIDH. The mitigations were proposed by a different team of researchers who independently discovered the same weakness. AMD declined to comment ahead of the lifting of a coordinated disclosure embargo.

24.Edward Snowden Believes Crypto Is Good For Payments, Not For Investments: Here's Why

by Shayak Majumder

https://news.abplive.com/business/crypto/edward-snowden-bitcoin-crypto-crash-price-good-for-payments-not-for-investments-coindesk-consensus-2022-1537261

Edward Snowden, the known NSA whistleblower, believes that cryptocurrencies may not be suitable for investments, but can provide more value when used for payments and similar services. Speaking virtually at CoinDesk's Consensus 2022 conference held in Austin, Texas, US, Snowden revealed how he prefers to use Bitcoin and explained what "distances" him from several other members of the global crypto community. The cryptocurrency market is facing an unprecedented plunge in prices, with Bitcoin registering a record 18-month low on Monday.

Snowden said at the CoinDesk event, "I use Bitcoin to use it. In 2013, Bitcoin is what I used to pay for the servers pseudonymously." In 2013, Snowden leaked classified information on how the US National Security Agency (NSA) snooped on citizens.

"Generally I don't encourage people to put their money in cryptocurrencies as a technology and this is what distances me from a lot of people in the community," Snowden added.

Snowden's statements come at a time when the overall crypto market is seeing unprecedented bloodshed in terms of prices. Bitcoin, the world's largest crypto, has been on a decline for 12 consecutive weeks now. At the time of writing, Bitcoin price stood at $22,375, as per CoinMarketCap data. This is more than half lesser than BTC's 2022 high of $49,000, and considerably lower than the crypto's all-time high of $68,000.

While Snowden didn't comment directly on the current market meltdown, his words do serve as a caution against crypto investors.

Considering the current market scenario, Edul Patel, CEO and Co-Founder of crypto trading platform Mudrex, told ABP Live, "investors looking towards stocking up on cryptos can DCA." For those unaware, DCA, or dollar-cost averaging, is a long-term strategy that can help reduce the impact of market volatility by investing smaller amounts into an asset on a regular basis.

"At the same time, others should closely monitor the market movements rather than jumping into impulsive buying activities," Patel added.

25.Top 63 Quantum Computer Simulators for 2022

by James Dargan
https://thequantuminsider.com/2022/06/14/top-63-quantum-computer-simulators-for-2022/

What are Quantum Computer Simulators?

The Quantum Insider believes it is time to provide a list detailing the top QC simulators for 2022. Non-exhaustive as usual, whether you are a quantum programmer, software developer or algorithm enthusiast, you will find a simulator—targeted for specific programming languages like C/C++, Java, Javascript, Julia, Maple, Mathematica, Maxima, Python etc.—to suit your needs.

We should make it clear that we have included software to simulate quantum effects in the list, too, as well as the simulators of quantum computers themselves.

After something in a similar vein? Then here is a link to the Top 35 Open Source Quantum Computing Tools [2022], published at the end of May of this year.

Before we go there, though, it's worth mentioning what a quantum computer simulator is. In a nutshell, a quantum computer simulator (also called a quantum circuit simulator) is a machine—or rather a device—that, according to T. H. Johnson et al in their paper What is a quantum simulator?, "actively use quantum effects to answer questions about model systems and, through them, real systems[...] reveal[ing] information about an abstract mathematical function relating to a physical model."

With that out of the way, I think it's time to go through some of the best out there in 2022:

1. **Intel Quantum Simulator (IQS, former qHiPSTER):** Available on GitHub, the Intel Quantum Simulator (Intel-QS), also known as qHiPSTER (The Quantum High-Performance Software Testing Environment), is a simulator of quantum circuits optimized to take maximum advantage of multi-core and multi-nodes architectures. It is based on a complete representation of the qubit state but avoids the explicit representation of gates and other quantum operations in terms of matrices. Intel-QS uses the MPI (message-passing-interface) protocol to handle communication between the distributed resources used to store and manipulate quantum states.

2. **staq:** Another simulator available as a GitHub repository, staq is a modern C++17 library for the

synthesis, transformation, optimization and compilation of quantum circuits authored by softwareQ Inc. under the MIT License. It is usable either through the provided binary tools or as a header-only library that can be included to provide direct support for parsing & manipulating circuits written in the OpenQASM circuit description language.

3. **QuEST:** QuEST is developed by Simon Benjamin's Quantum Technology Theory Group (qtechtheory) and the e-Research center (oerc) at the University of Oxford. Development is currently led by Tyson Jones.

4. **Scaffold/ScaffCC:** ScaffCC is a compiler and scheduler for the Scaffold programing language. It is written using the LLVM open-source infrastructure. It is for the purpose of writing and analyzing code for quantum computing applications.

5. Qrack: Qrack is a C++ quantum bit and gate simulator, with the ability to support arbitrary numbers of entangled qubits—up to system limitations. Suitable for embedding in other projects, the Qrack QInterface contains a full and performant collection of standard quantum gates, as well as variations suitable for register operations and arbitrary rotations.

6. **QX Simulator:** The QX Simulator is a universal quantum computer simulator developed at QuTech by Nader Khammassi. The QX allows quantum algorithm designers to simulate the execution of their quantum circuits on a quantum computer. The simulator defines a low-level quantum assembly language namely Quantum Code which allows the users to describe their circuits in a simple textual source code file. The source code file is then used as the input of the simulator which executes its content.

7. **Quantum++:** Available as a GitHub repository, Quantum++ is a modern C++ general-purpose quantum computing library, composed solely of template header files. Quantum++ is written in standard C++17 and has very low external dependencies, using only the Eigen 3 linear algebra header-only template library and, if available, the OpenMP multi-processing library.

8. **LanQ:** LanQ is a research project in the field of quantum computer science—a quantum programming language designed to support the execution of multiple processes in parallel with a syntax similar to the C language.

9. **libquantum:** libquantum is a C library for the simulation of quantum mechanics, with a special focus laid on quantum computing. It started as a pure quantum computer simulator, but support for general quantum simulation has been recently added. Based on the principles of quantum mechanics, libquantum provides an implementation of a quantum register. Basic operations for register manipulation such as the Hadamard gate or the Controlled-NOT gate are available through an easy-to-use interface. Measurements can be performed on either single qubits or the whole quantum register.

10. **QDD:** QDD is a C++ library which provides a relatively intuitive set of quantum computing constructs within the context of the C++ programming environment. QDD is unique in that its emulation of quantum computing is based upon a Binary Decision Diagram (BDD) representation of the quantum state. This is in contrast to the complex number representation used by QCL and Open QuBit.

11.**qsims:** qsims was developed as a tool for studying quantum computing in addressable optical lattices. It is a general-purpose quantum simulation software package, capable of simulating the dynamics of systems with a wide range of Hamiltonians. qsims is by no means limited to optical lattices and could be adapted for use in many other physical systems, or for use as a teaching tool.

12.**Quantum Computer Language (QCL):** QCL is a programming language for quantum computers. Despite many common concepts with classical computer science, quantum computing is still widely considered a special discipline within the broad field of theoretical physics. One reason for the slow adoption of QC by the computer science community is the confusing variety of formalisms (Dirac notation, matrices, gates, operators, etc.), none of which has any similarity with classical programming languages, as well as the rather "physical" terminology in most of the available literature.

13.**Qubiter:** Qubiter 1.11 is a free computer program pertaining to quantum computers (QC) and quantum Bayesian (QB) nets. Currently, Qubiter is available only as pure C++ source code, without a graphical user interface.

14.**QuCoSi:** QuCoSi is a C++ library for simulating a quantum computer. The used qubits and gates are plain vectors and matrices that can be inspected and modified easily. Its emphasis lies in readability and ease of use.

15.**QuIDDPro:** QuIDDPro is a fast, scalable, and easy-to-use computational interface for generic quantum circuit simulation. It supports state vectors, density matrices, and related operations using the Quantum Information Decision Diagram (QuIDD) data structure. Software packages including Matlab, Octave, QCSim, and libquantum, have also been used to simulate quantum circuits. However, unlike these packages, QuIDDPro does not always suffer from the exponential blow-up in size of the matrices required to simulate quantum circuits. As a result, we have found that QuIDDPro is significantly faster and uses significantly less memory as compared to other generic simulation methods for some useful circuits with many more than ten qubits

16.**QWalk:** QWalk is a free simulator of quantum walks for one- and two-dimensional lattices. The simulator can be easily compiled in Linux or any other similar operating system with a recent C compiler.

17.**sqct—Single qubit circuit toolkit:** sqct is a software package for the exact and approximate synthesis of single-qubit circuits using Clifford and T gate library.

18.**MQT-DDSIM (previously JKQ-DDSIM):** MQT DDSIM is a quantum circuit simulator based on decision diagrams written in C++. A tool for classical-quantum circuit simulation by the Chair for Design Automation at the Technical University of Munich, QCEC is part of the Munich Quantum Toolkit (MQT; formerly known as JKQ and developed by the Institute for Integrated Circuits at the Johannes Kepler University Linz). It builds upon our quantum functionality representation (QFR) and our decision diagram (DD) package.

19.**LIQUi|>:** LIQUi|> is a software architecture and tool suite for quantum computing. It includes a programming language, optimization and scheduling algorithms, and quantum simulators. LIQUi|> can be used to translate a quantum algorithm written in the form of a high-level program into the low-level machine instructions for a quantum device. LIQUi|> is being developed by the Quantum Architectures and Computation Group (QuArC) at Microsoft Research.

20. **Quantum Programming Studio:** The Quantum Programming Studio is a web-based graphical user interface designed to allow users to construct quantum algorithms and obtain results by simulating directly in the browser or by executing on real quantum computers.

21. **Qubit Workbench:** Qubit Workbench, from quantum startup Elyah, allows users to take quantum algorithm design to a new level with an all-new IDE experience with a web-based IDE and Simulator, drag and drop circuit builder, and printable circuits.

22. **Linear AI:** Linear AI is a multi-purpose research, design and teaching tool for quantum information processing. It supports many of the mathematical structures commonly used in the field with notation designed for use by quantum information scientists.

23. **QCAD:** QCAD is a Windows-based environment for quantum computing simulation which helps users design circuits and simulate them. QCAD enables you to design quantum circuits easily with a full GUI (graphical user interface) environment and simulate the designed circuit and show results (states of qubits).

24. **Quantum Computer Emulator:** The Quantum Computer Emulator (QCE) is a software tool that emulates various hardware designs of quantum computers. QCE simulates the physical processes that govern the operation of a hardware quantum processor, strictly according to the laws of quantum mechanics. QCE also provides an environment to debug and execute quantum algorithms under realistic experimental conditions. The software consists of a Graphical User Interface (GUI) and the simulator itself.

25. **Quantum Fog:** Quantum FogTM (US Patent 5787236) is a Mac application for modelling physical situations that exhibit quantum mechanical behaviour. It's a tool for investigating and discussing quantum measurement problems graphically, in terms of network diagrams called quantum Bayesian nets. It can calculate one- and two-variable conditional probability distributions, and it can draw a picture of every Feynman path that contributes to a physical situation. It simulates a general-purpose quantum computer.

26. **SimQubit:** SimQubit is a GUI quantum circuit simulator, written on top of the Q++ (sourceforge.net/projects/qplusplus) quantum templates. It allows editing of quantum circuits and applying them to quantum states, with multiple ways to view the output probabilities.

27. **Q-Kit:** Q-Kit—or Quantum-Kit—is a graphical quantum circuit simulator. Q-Kit enables building and designing quantum circuits, visualizing the effect of quantum gate operations as probability distributions of quantum states or on a Bloch Sphere.

28. **jQuantum — Quantum Computer Simulator:** jQuantum is a program which simulates a quantum computer. Users can design quantum circuits with it and let them run. The aim of jQuantum is to enable development as well as demonstrations of quantum algorithms.

29.**QuanSuite:** QuanSuite is a suite of Java applications, available for free. QuanSuite application compiles a different kind of input evolution operator Uin. The applications output a quantum circuit for Uin, where Uin is specified either directly, or by giving a Hamiltonian H such that Uin=exp(iH).

30.**Quantomatic:** Quantomatic is a diagrammatic proof assistant, meaning it provides machine support for reasoning with diagrammatic languages (check out some of our papers). It allows users to draw diagrams and build up proofs using diagrammatic rewrite rules.

31.**Qubit101:** The Qubit101 simulator is a user-friendly quantum circuit editor and simulator. The tool helps users to create, modify and save the quantum circuits. Along with this, users can simulate its effect over a predefined quantum state, watch the evolution of the state stage by stage, together with the possible measurements results, use other quantum circuits as gates, so complex circuits can be easily created and finally, simulate an almost arbitrary number of qubits.

32.**QuSAnn (and Multiplexor Expander):** QuSAnn v1.2 and Multiplexor Expander v1.2 are two Java applications available for free. (Source code included in the distribution.) QuSAnn is a "code generator" for quantum simulated annealing: after the user inputs some parameters, it outputs a quantum circuit for performing simulated annealing on a quantum computer. The quantum circuit implements the algorithm of Wocjan et al.(arXiv:0804.4259), which improves on the original algorithm of Somma et al.(arXiv:0712.1008). The quantum circuit generated by QuSAnn includes some quantum multiplexors. The application Multiplexor Expander allows the user to replace each of those multiplexors with a sequence of more elementary gates such as multiply controlled NOTs and qubit rotations.

33.**Strange:** A quantum simulator with an API and a link to a JavaFX visualiser, Strange is distributed via the traditional Java distribution channels (e.g. maven central and jcenter) and can thus easily be used leveraging maven or gradle build software.

34.**Quantum Computer Simulator:** The Quantum Computer Simulator is what's known as an "ideal quantum computer," meaning that any and all qubits can be entangled and qubits don't collapse from superposition unexpectedly. A real quantum computer has physical limitations on which qubits can be entangled and for how long superposition states can be maintained. The code you write here may need to be altered slightly to work on a real quantum computer.

35.**quantum-circuit — Quantum circuit simulator implemented in javascript:** The quantum-circuit is an open-source quantum circuit simulator implemented in javascript. Smoothly runs 20+ qubit simulations in the browser or at the server (node.js). You can use it in your javascript program to run quantum simulations.

36.**jsqis: Javascript Quantum Information Simulator:** jsqis, at its core, is a quantum computer simulator written in Javascript. It allows the initialization of quantum registers and their manipulation by means of quantum gates.

37.**QSWalk.jl:** QSWalk provides a package for Julia programming language which enables high-performance analysis of quantum stochastic walks. There are two main advantages of the presented packages over the existing software. First, it can be used to describe quantum stochastic walks in the local, as well as global regime. Second, it enables the user to seamlessly utilize parallel computing capabilities.

38. QuantumOptics.jl: QuantumOptics.jl is a numerical framework written in the Julia programming language that makes it easy to simulate various kinds of open quantum systems. It is inspired by the Quantum Optics Toolbox for MATLAB and the Python framework QuTiP.

39. QuantumWalk.jl: QuantumWalk.jl is a package for Julia programming language implementing models of quantum continuous and discrete walks used for performing a quantum spatial search. Its main purpose is to provide general functionalities by crossing the usage of quantum models and application implementations.

40. Yao.jl: Yao.jl is an open-source framework that aims to empower quantum information research with software tools, quantum algorithm design, quantum software 2.0, and quantum computation education.

41. Quantum: Quantum is a free Mathematica add-on for Dirac Bra-Ket Notation, Quantum Algebra, Quantum Computing and the QHD approximation to the Heisenberg Equations of Motion authored by by José Luis Gómez-Muñoz and Francisco Delgado from the Tecnológico de Monterrey.

42. QuantumUtils: Available as a GitHub repository, QuantumUtils for Mathematica is a software library for quantum information scientists facilitating symbolic and numerical calculations, with extensive documentation.

43. Quantum Information Programs in Mathematica: Quantum Information Programs in Mathematica has a collection of functions and other objects useful for simulating small quantum circuits using Mathematica. It is intended for tinkerers: users who want to set up and modify their own simulation programs using Mathematica, but do not have the time or inclination to develop everything from scratch. The documentation provides a description of how the system works, along with a simple example.

44. QI: A GitHub repository, QI is a package for Mathematica computer algebra system developed to support symbolic analysis of quantum states and operations.

45. qinf: qinf is a quantum information package for the Maxima computer algebra system by John Lapeyre, a Quantum Software Engineer at Rigetti Computing.

46. M-fun for QC Progs: M-fun for QC Progs (Matlab Functions—and fun—for Quantum Computer Programmers), by R.R.Tucci, is a toolbox of Octave/MATLAB m-files for QC programming

47. QETLAB: QETLAB (Quantum Entanglement Theory LABoratory) is a MATLAB toolbox for exploring quantum entanglement theory. While there are many quantum information theory toolboxes that allow the user to perform basic operations such as partial transposition, new tests are constantly discovered. The goal of QETLAB is to remain up-to-date and contain an ever-growing catalogue of separability criteria, positive maps, and related functions of interest.

48. QLib: QLib is a Matlab package intended to provide a wide audience within the QIT community

with the tools needed to accelerate research by quickly and efficiently framing and exploring questions, forming intuition through the use of visualizations, ruling-out or validating hypotheses through the use of optimization.

49. **Qubit4matlab:** QUBIT4MATLAB is a MATLAB package for quantum information/quantum optics written by Geza Toth.

50. **Quantum.NET:** Quantum.NET is a library to manipulate qubits and simulate quantum circuits.

51. **Quirk:** Quirk is a drag-and-drop quantum circuit simulator that runs in your browser, with no installing or configuring or scripting. A toy for exploring and understanding small quantum circuits, especially if you want to quickly explore the behaviour of a small quantum circuit.

52. **QRBGS (Quantum Random Bit Generator):** QRBG has been motivated by scientific necessity (primarily of the local scientific community) of running various simulations (in cluster/Grid environments), whose results are often greatly affected by the quality (distribution, nondeterminism, entropy, etc.) of used random numbers. Since true random numbers are impossible to generate with a finite state machine (such as today's computers), scientists are forced to either use specialized expensive hardware number generators or, more frequently, to content themselves with suboptimal solutions (like pseudo-random numbers generators).

53. **PyQu:** PyQu is an extension module for Python to implement quantum algorithms and is an extension module for Python 3 whose main goal is to provide a complete set of data types and functions for simulating quantum computation with a neat syntax. PyQu is written in C and makes extensive use of libquantum-1.0.0 library by Björn Butscher and Hendrik Weimer. However, PyQu intends not to be just a wrapper of libquantum to Python, but rather a new high-level language (in Python style of course) for quantum programming.

54. **Qiskit:** Qiskit is an open-source SDK for working with quantum computers at the level of pulses, circuits, and application modules developed by IBM Research and the Qiskit community.

55. **qitensor:** qitensor is a python module for quantum information and map-state duality, matrix-level quantum operations, with labelled component Hilbert spaces.

56. **QuaEC:** QuaEC is a library for working with quantum error correction and fault tolerance in Python. In particular, QuaEC provides support for manipulating Pauli and Clifford operators, as well as binary symplectic representations of each.

57. **sparse_pauli:** The implementation of large, sparse Pauli operators using pairs of sets. Contains absolutely minimal functionality, and is an example of extreme "physicist code".

58. **toqito:** toqito is an open-source Python library for studying various objects in quantum information.

59. **OpenQASM:** OpenQASM is an imperative programming language for describing quantum circuits. It is capable to describe universal quantum computing using the circuit model, measurement-based

model, and near-term quantum computing experiments, released as part of IBM's QISKit.

60. **VQS—Visual Quantum Simulator:** VQS (Visual Quantum Simulator) is a universal Schrödinger full state Quantum Simulator, designed as a Scala DSL

61. **QIO:** The Quantum IO Monad is a library for defining quantum computations in Haskell. It can be thought of as an embedded language within Haskell, and comes with functions for simulating the running of these quantum computations. The distribution contains many example computations written in QIO, including the implementation of Shor's algorithm.

62. **Quipper:** Quipper is an embedded, scalable functional programming language for quantum computing. It provides a high-level circuit description language—this includes gate-by-gate descriptions of circuit fragments, as well as powerful operators for assembling and manipulating circuits, a syntax that allows a mixture of procedural and declarative programming styles, and built-in facilities for the automatic synthesis of reversible quantum circuits, including from classical code.

63. **qchas:** qchas is a library useful for implementing quantum algorithms. It contains definitions of quantum gates and qubits written in Haskell.

26. Hello XD ransomware now drops a backdoor while encrypting

by Bill Toulas
https://www.bleepingcomputer.com/news/security/hello-xd-ransomware-now-drops-a-backdoor-while-encrypting/

Cybersecurity researchers report increased activity of the Hello XD ransomware, whose operators are now deploying an upgraded sample featuring stronger encryption.

First observed in November 2021, the particular family was based on the leaked source code of Babuk and engaged in a small number of double-extortion attacks where the threat actors stole corporate data before encrypting devices.

According to a new report by Palo Alto Networks Unit 42, the malware's author has created a new encryptor that features custom packing for detection avoidance and encryption algorithm changes.

This marks a significant departure from the Babuk code and highlights the author's intention to develop a new ransomware strain with unique capabilities and features for increased attacks.

Hello XD ransomware operation

The Hello XD ransomware operation is not currently using a Tor payment site to extort victims but instead instructs victims to enter negotiations directly through a TOX chat service.

In the latest version, the malware operators have added an onion site link on the dropped ransom note, but Unit 42 says the site is offline, so it might be under construction.

When executed, Hello XD attempts to disable shadow copies to prevent easy system recovery and then encrypts files, adding the **.hello** extension to file names.

Besides the ransomware payload, Unit 42 also observed Hello XD operators now using an open-source backdoor named MicroBackdoor to navigate the compromised system, exfiltrate files, execute commands, and wipe traces.

This MicroBackdoor executable is encrypted using WinCrypt API and embedded within the ransomware payload, so it's dropped to the system immediately upon infection.

Crypter and encryption

The custom packer deployed in the ransomware payload's second version features two layers of obfuscation.

The author has derived the crypter by modifying UPX, an open-source packer that numerous malware authors have widely abused in the past.

The embedded blobs decryption involves using a custom algorithm containing unconventional instructions like XLAT, while the API calls in the packer are weirdly not obfuscated.

The most interesting aspect of the second major version of Hello XD is switching the encryption algorithm from modified HC-128 and Curve25519-Donna to Rabbit Cipher and Curve25519-Donna.

Additionally, the file marker in the second version was changed from a coherent string to random bytes, making the cryptographic result more powerful.

What we should expect

At this time, Hello XD is a dangerous early-stage ransomware project currently being used in the wild. Even though its infection volumes aren't significant yet, its active and targeted development lays the ground for a more dangerous status.

Unit 42 traced its origins to a Russian-speaking threat actor using the alias **X4KME**, who uploaded tutorials on deploying Cobalt Strike Beacons and malicious infrastructure online.

Additionally, the same hacker has posted on forums to offer proof-of-concept (PoC) exploits, crypter services, custom Kali Linux distributions, and malware-hosting and distribution services.

All in all, the particular threat actor appears knowledgeable and in a position to move Hello XD forward, so analysts need to monitor its development closely.

27.China allegedly made a breakthrough in protecting blockchains from quantum attacks

by Christopher McFadden
https://interestingengineering.com/china-protecting-blockchains-quantum-attacks

According to the state-owned China News Service, the Chinese blockchain platform ChainMaker has been built with technology that can withstand assaults from both conventional and quantum computers.

A blockchain, in case you are unaware, is a digital ledger that keeps track of all transactions.

According to the news agency, developers of the business blockchain, also known as Chang'An Chain, claimed the new technology safeguards information transfer between financial institutions, making online transactions safer.

The Beijing Academy of Blockchain and Edge Computing designed the system, which was introduced in January of last year. It is China's first autonomous blockchain platform and was created in collaboration with universities such as Tsinghua and Beihang, as well as IT heavyweights like Tencent and Baidu.

According to the China News Service report, a post-quantum digital signature method has been added to the blockchain platform to protect it against assaults, including those by quantum computers, which might jeopardize the security of regular communications.

The Chinese blockchain uses some very smart algorithms to counter quantum threats

Like other blockchains, the digital list of records is maintained in blocks, each including the transaction time and date, and is meant to be difficult to update without being discovered.

Transactions involve the use of cryptographic hash functions or challenging math problems, as well as "proof-of-work" problems that validate each block that came before it to guarantee the list remains safe.

In 1994, US mathematician Peter Shor discovered that a quantum computer might be used to calculate the prime factors of large numbers. This lit the spark for the inevitable decline of conventional secure communications that utilize encryption based on computational complexity.

In response to this, classic cryptographic techniques, dubbed "post-quantum cryptography", as well as a quantum key distribution scheme, have been designed to fight possible quantum computer assaults.

To this end, the president of quantum tech company QuantumCTek told state-run China Science Daily that developing solutions to prevent quantum assaults is critical, even if a full-fledged quantum computer may take another eight to ten years to build.

On Monday, the company's director, Ying Yong, was cited as stating, "The cost of making amends will be huge - we should plan ahead."

"Building a quantum secure communication network is an urgent matter. The denser the network, the better; and the denser it is, the more practical it becomes," he added.

While blockchains are most widely utilized through peer-to-peer networks to verify decentralized data—generally for managing cryptocurrency, they are also used in China to verify contracts, health data, and other types of data. In fact, it is similar functions that are the real potential for the technology, rather than the plethora of digital coins that tend to dominate the news cycle.

During the Beijing Winter Olympics earlier this year, ChainMaker said that its technology was utilized in carbon trading, supply chain financing, and food origin tracking.

According to the official Chinese broadcaster CCTV, the consortium said in June last year that it had installed a 96-core blockchain processor that makes signature verification 20 times quicker and smart contract processing 50 times faster on the network.

28.Theory suggests quantum computers should be exponentially faster on some-learning tasks than classical machines

by Bob Yirka

https://phys.org/news/2022-06-theory-quantum-exponentially-faster-tasks.html

A team of researchers affiliated with multiple institutions in the U.S., including Google Quantum AI, and a colleague in Australia, has developed a theory suggesting that quantum computers should be exponentially faster on some learning tasks than classical machines. In their paper published in the journal Science, the group describes their theory and results when tested on Google's Sycamore quantum computer. Vedran Dunjko with Leiden University City has published a Perspective piece in the same journal issue outlining the idea behind combining quantum computing with machine learning to provide a new level of computer-based learning systems. Machine learning is a system by which computers trained with datasets make informed guesses about new data. And quantum computing involves using sub-atomic particles to represent qubits as a means for conducting applications many times faster than is possible with classical computers. In this new effort, the researchers considered the idea of running machine-learning applications on quantum computers, possibly making them better at learning, and thus more useful.

To find out if the idea might be possible, and more importantly, if the results would be better than those achieved on classical computers, the researchers posed the problem in a novel way—they devised a machine learning task that would learn via experiments repeated many times over. They then developed theories describing how a quantum system could be used to conduct such experiments and to learn from them. They found that they were able to prove that a quantum computer could do it, and that it could do it much better than a classical system. In fact, they found a reduction in the required number of experiments needed to learn a concept to be four orders of magnitude lower than for classical systems. The researchers then built such a system and tested it on Google's Sycamore quantum computer and confirmed their theory.

The work suggests that if a usable, real-word quantum computer is ever developed, it might be capable of leaning new things on a nearly unimaginable scale.

29.Privacy depends on cybersecurity — why government must rethink the new rules

by Apar Gupta

https://www.thehindu.com/opinion/op-ed/privacy-depends-on-cybersecurity-why-government-must-rethink-the-new-rules/article65513469.ece

While increasing surveillance, the directions issued by CERT-In present few, if any, benefits for security of the state or individuals.

If you had to choose between privacy and security, which would you prefer? While the answer may lean towards security for many, imagine losing out on both. This is likely to be the fallout of **directions issued by the Indian Computer Emergency Response Team** (CERT-In) on April 28, 2022.

Let's first cover the basics. CERT-In is a body established under the Information Technology Act, 2000 tasked with the broad mandate of "securing Indian cyberspace", and reports to the Ministry of Electronics and IT (MEITY). With ubiquitous digitisation, cyber security has gained prominence in recent years. For instance, as per a parliamentary response CERT-In reported an almost nine-fold increase over six years to a total of 48,285 cyber security incidents related to government authorities. It mirrors the experience of users and the private sector who feel unsafe with their personal data being routinely breached, often leading to cyber crime. As per the Crime In India report in 2020, there has been an **almost 12% rise in cyber crimes,** with the large majority clustered in the categories of fraud, sexual exploitation and extortion. These are serious consequences for national and user security that increase the importance of CERT-In's mission.

Woefully, the directions issued by CERT-In, while increasing surveillance, present few, if any, benefits for security of the state or individuals. These directions go into effect on June 27, 2022, and have six operative provisions whose violation carries a one-year term of imprisonment. While much of the concern has arisen from users of Virtual Private Networks (VPNs), the directions go much further.

Synchronisation, immediate reporting

Let us deal with each direction individually, starting with the requirement for all service providers to connect their system clocks to the network time protocol servers of the government. On the face of it, this is a welcome move, as all computer systems contain logs which require verifiable timestamps. However, by linking them to government servers, security experts have observed that it creates a single point of failure and increases the attack surface for a supply chain attack.

The second direction requires all service providers to inform CERT-In whenever any "cyber incidents" occur, within six hours of gaining knowledge. This is again another direction which is positive at first glance, as it indicates that the government will now need to be informed any time there is a data breach rather than the information being tucked away in a corporation's black box. However, there are core deficiencies which undermine the positives. One, "cyber incident" is not properly defined and makes reference to vague categories such as "fake mobile apps". Even routine events such as "unauthorized access to social media accounts" will need to be reported. This will not only increase the reporting burden of system administrators, but flood CERT-In with notifications beyond their response capacity. Furthermore, there is no obligation on CERT-In to inform users who are ultimately at risk. There is no mention of what actions CERT-In must take and how its actions will be publicly disclosed. Reporting "cyber incidents" is also an incomplete measure, given there is no provision for penalties and fines on the public or private sector.

Real-time information

The third direction enhances the power of CERT-In to seek information from service providers by extending them to "protective and preventive actions". Again, there is little transparency on how CERT-In will exercise this power which now includes seeking "real time" information that could be used for the purpose of surveillance. Quite simply, CERT-In can direct any system provider even without a security incident occurring, with little oversight, and seek any data. Such surveillance fears become obvious when we look at the next two directions.

Imagine that each online service provider will now maintain and store logs of all your online activity for 180 days and store them within India. This is not all — some, including data centres and VPNs, will be required to mandatorily register users. These two directions have gathered the **bulk of public criticism from many users of VPNs**. VPNs provide a tunnel for online activity in which a user first plugs into a VPN server that in turn fetches information from the Internet. Hence, all it shows to an Internet service provider such as Airtel or Jio, or even the websites a user visits, is the connection and address of the VPN server. This permits accessing blocked content, geolocating to another country or also, as claimed, surfing the Internet without logging. While the privacy claims of VPN providers are contentious, according to the Freedom of the Press Foundation if chosen well they "offer key security benefits to your workflow". All of this will be a thing of the past with the mandate to store logs, that will essentially mean that whether you are a VPN user or not, each service provider will be required to collect and store more personal data of users. This may result in zero knowledge services such as messaging applications like Signal or secure browsing technologies like Tor being blocked in India. In addition to this, providers will now need to mandatorily register users on seven data points like a bank's KYC process and store it for five years. This is a tremendous expansion in data collection which will match a person's online activity with their real world identity.

The government response

The response to the public criticism has been worrying. The Minister for State for Electronics and IT has in press statements stated that VPN providers should **comply with the directions or leave India**. These remarks were made alongside the release of a "Frequently Asked Questions (FAQ)" document released on May 18, 2022 that changed little and failed to provide many answers. As per the Ministry itself, this document does not have any legal effect, and hence any clarifications will be left to discretionary practices. While such flexibility is beneficial for the government, it could certainly result in arbitrary and unequal enforcement. Furthermore, the increase in personal data being collected of users without a data protection law will increase risks to individual users if such data is breached.

This complementary relationship between maintaining privacy and security is explained at length by Laura DeNardis in The Internet is Everything when she states, "The considerable amount of data collected also creates a target for data thieves and identity theft and also a target for direct harm to particular individuals…. Privacy depends on cybersecurity ." Oblivious to reason, the CERT-In directions offer security for our privacy, but end up hurting both.

30.Data Is Vulnerable to Quantum Computers That Don't Exist Yet

by Charles Q. Choi
https://spectrum.ieee.org/post-quantum-cryptography

Future quantum computers may rapidly break modern cryptography. Now a new spin-off from Google's parent company Alphabet warns that sensitive data is already vulnerable to quantum computers that don't exist yet, courtesy of codebreaking attacks that steal that data now and could decrypt it in the future. Therefore, it has developed a road map to help businesses, governments and other organizations begin the shift to post-quantum cryptography now.

The new startup, Sandbox AQ (which stands for AI and quantum), has already attracted clients including Mount Sinai Health System, telecommunications firm Softbank Mobile, communications technology company Vodafone Business, and Web developer Wix. It has also reeled in investors including the

CIA's venture capital arm In-Q-Tel and cybersecurity-focused investment firm Paladin Capital Group. Former Google CEO Eric Schmidt is serving as the chairman of its board of directors.

In addition, Sandbox AQ has already partnered with two of the world's largest professional service firms, Ernst & Young and Deloitte, to help deploy post-quantum cryptography.

"These firms have the scale to educate, engage, and upgrade post-quantum cryptography for their Global 1000 clients, which represent the world's largest and most successful companies," says David Joseph, a research scientist at Sandbox AQ in Palo Alto, Calif. "Doing this will multiply the impact of our quantum solutions and help companies protect their customers, data, networks, and other assets today, without having to wait until error-corrected quantum computers become available."

Quantum computers theoretically can quickly solve problems it might take classical computers untold eons to solve. For example, much of modern cryptography depends on the extreme difficulty that classical computers face with regard to mathematical problems such as factoring huge numbers, but quantum computers could in principle rapidly crack even highly secure RSA-2048 encryption. To stay ahead of quantum computers, scientists around the world have spent the past two decades designing post-quantum cryptography (PQC) algorithms. These are based on new mathematical problems that both quantum and classical computers find difficult to solve. In January, the White House issued a memorandum on transitioning to quantum-resistant cryptography, underscoring that preparations for this transition should begin as soon as possible.

However, after organizations such as the National Institute of Standards and Technology (NIST) help decide which PQC algorithms should become the new standards the world should adopt, there are billions of old and new devices that will need to get updated. Sandbox AQ notes that such efforts could take decades to implement.

Although quantum computers are currently in their infancy, there are already attacks that can steal encrypted data with the intention to crack it once codebreaking quantum computers become a reality. Therefore, the Sandbox AQ argues that governments, businesses, and other major organizations must begin the shift toward PQC now.

For example, in a store-now-decrypt-later attack, adversaries would capture precious encrypted information now, store it, and decrypt it when practical quantum computers exist. Stolen data could include medical records, national security documents, trade secrets, and more—any information that may still prove valuable even decades later.

"We know for a fact that store-now-decrypt-later attacks are happening right now, and their frequency will only increase the closer we get to delivering a fault-tolerant quantum computer," Joseph says. "Once encrypted data has been exfiltrated, there is no way to protect it from future decryption and exploitation."

Store-now-decrypt-later attacks do not need high-profile breaches to succeed. "They could be performed silently by first observing encrypted data on public networks, which would be very difficult to detect," Joseph says. "Over the public Internet, encrypted data might be sent via many different nodes, and any one of these nodes could be compromised, copying and storing valuable data before forward-ing it on to its intended final destination."

The main difficulty in executing store-now-decrypt-later attacks is figuring out which data to target, "as there will be an enormous volume of encrypted data and only a finite amount of quantum computing resources," Joseph says. "We expect the first quantum-enabled adversaries will be nation-states, and it may not be public knowledge exactly when one of them gains access to a large, fault-tolerant device capable of breaking RSA-2048."

Another reason shifting to post-quantum cryptography may prove important is because of projects that are getting designed and planned now but may have life spans of decades, such as many cars, planes, trains, and ships in production now, or critical national infrastructure projects. The hardware needed to implement cryptography may essentially remain immutable for the lifetime of these products and projects, so the earlier they can get protected, the better, Joseph and his colleagues note.

The inspiration to launch Sandbox AQ grew from discussions between security teams within Alphabet starting from 2016.

"It became apparent that there was a huge wealth of experience across the now-Sandbox AQ team and the Googlers across Alphabet, but most of this expertise was focused on distinct, introspective efforts that directly benefited Google's customers," Joseph says. "However, when we spoke with decision-makers at external organizations, it became clear that what was 'common knowledge' in the security community was not well known at large."

Sandbox AQ's efforts to explain the importance of PQC led the startup to draft a new road map for organizations to shift past traditional cryptography. The company detailed its road map on 11 May in the journal Nature.

The first recommendation Sandbox AQ makes is to figure out where PQC transition is needed first. The workforce to perform these upgrades is highly specialized and usually scarce, and so needs to get deployed in ways that make the most of resources to protect systems best. This involves identifying the cryptographic schemes that are at highest risk, such as key exchange algorithms, the kind that often underlie secure messages and data transfers.

Instead of replacing existing algorithms with relatively untested PQC alternatives, the road map notes that scientists have developed hybrid algorithms combining both traditional algorithms and post-quantum algorithms. Therefore, even if the PQC algorithm later proves flawed, at least the classical algorithm can still provide a measure of security.

The road map notes that NIST's PQC project is close to the end of its third round and standards for the algorithms selected are expected to be released no later than 2024. Sandbox AQ recommends that organizations may want to start experimenting now with the finalist and alternative candidates. The company also suggests considering stateful hash-based signature technology for applications such as software code signing, as NIST and other bodies have already standardized it.

The most comprehensive repository of the software implementations of the NIST schemes is Liboqs of the Open Quantum Safe project. Other resources include BoringSSL, Tink, and SUPERCOP.

Due to the current diversity of PQC alternatives, the need to change from one algorithm to another in case of a successful attack, and the desire for increasing connectedness between systems, the road map also recommends "crypto-agility," or the ability to switch between cryptographic schemes. Sandbox AQ notes that standards bodies should make 6G wireless technologies, for example, inherently crypto-agile and PQC-compatible.

Sandbox AQ also helps organizations shift to PQC by conducting three-phase security audits. "The first phase is discovery, where we assess and catalog the organization's cryptographic infrastructure to understand where any potential vulnerabilities lie," Joseph says. "We then conduct a performance analysis in order to provide a quantum readiness evaluation and risk-based PQC migration plan."

The next step "is the assessment phase, migrating selected candidates from IT infrastructure to demonstrate functional success and performance," he says. "We catalog mitigation patterns that will become the standard for the full implementation."

Finally comes "the implementation phase, which includes the complete transition of an organization's IT infrastructure, in order of priority," Joseph says. "It enables cryptographic agility throughout the network and enables full sovereignty over cryptographic usage."

As dangerous as code breaking quantum computers may prove, history shows that cryptography transitions need a considerable amount of time. For example, elliptic curve cryptography was proposed in the 1980s, and despite the fact that it is far more efficient than RSA in terms of space and speed, it took more than two decades to finally gain widespread adoption.

"By comparison, the transition to PQC will be larger and more complex," Joseph says. "From this frame of reference, it became clear that awareness needs to be increased and the transition process needs to start now."

31.What's the current state of quantum computing?

by Paul Nashawaty

https://www.techtarget.com/searchdatacenter/opinion/Whats-the-current-state-of-quantum-computing

Many large tech companies have already invested heavily in quantum technologies, yet significant adoption of quantum computing has had its share of delays and false starts. However, with some recent announcements in the quantum sector, now seems to be the ideal time for organizations to take a closer look at quantum and consider how this approach could work for their business workloads. Organizations that have been historically focused on classical computing are now positioning quantum for the future.

In an ESG IT spending survey, 11% of respondents indicated their organizations were piloting quantum for a few applications, 17% indicated they are testing and 24% of respondents have begun research but are years away from production apps. Finally, 27% have expressed an interest in quantum computing but have not taken any action toward embracing it.

This slow growth in adoption is about to change -- and possibly quickly. As leading organizations explore new ways to produce faster results, accelerate buying cycles and improve performance, they have become more open to shifting away from purely classical solutions to accelerate adoption of quantum.

The dynamic shift and market alignment

The industry is also discovering new methods and use cases that can be applied from classical to quantum computing platforms. Take, for example, the recent merger between Quantum Computing Inc. (QCI) and QPhoton, a quantum photonics company. Bill McGann, COO and CTO at QCI, discussed the merger.

Based on the information he shared, it seems that the combination of QCI and QPhoton capabilities can deliver a quantum computer that makes quantum systems more accessible for organizations, so they can see business results faster and more cost effectively. Another benefit of this merger is that the companies are broadening the user base to non-quantum experts, many of whom have been anxiously awaiting the opportunity to explore quantum-possible problems in areas like analytical optimization and drug discovery.

Using a full-stack approach, QCI and QPhoton together offer a unique opportunity to accelerate the delivery of practical quantum applications. This is the same process that drove value in classical computing. The merger of the two companies extends the QCI portfolio to help accelerate the accessibility of quantum computing for today's use cases, such as AI and optimization. This also enables quantum computing to operate at room temperatures, which is often a challenge with this type of computing.

Classical vs Quantum use cases

When it comes to the finance use case, one way to understand how to pivot from classical to quantum computing is to think through how algorithms work.

For example, take a traditional investor model. With a financial algorithm, you must understand and look at predefined user parameters, such as investment goals, risk tolerances and diversity of funds. In this scenario, the investor wants to understand the user's investment preferences and risk tolerances. This data is "parameterized" -- meaning variables are created and passed on to the quantum computing model, which could use an artificial intelligence model employed by the quantum-compliant Monte Carlo algorithm or other techniques to process the investor's instructions, analyze the global asset-universe stochastic data and produce corresponding investor-inquiry output results.

Another emerging focus or concept coming out of the investor model is enabling users to autonomously process and analyze stochastic financial asset data. An interface -- proprietary or not -- could enable users to provide predefined input parameters representing their investment preferences and risk-tolerance levels, and then produce independent customized solutions for each user.

Depending on the type of user inquiry or request for analysis, a version of AI -- such as autonomous dispersion analytics or autonomous diversification and allocation machine learning -- could deploy to process the instructions and analyze asset stochastic data. This process would be very difficult to achieve in classical computing environments.

Quantum: On the horizon

As IBM chief quantum exponent Robert Sutor explained in a blog post from last July, "Quantum computers will solve some problems that are completely impractical for classical computers." This indicates that organizations plan to adopt quantum into their existing environments.

"[QCI is committed to be the] democratizing force that empowers non-quantum experts to realize quantum value," said Robert Liscouski, CEO of QCI. The recent acquisition of QPhoton accelerates this ease-of-use approach.

Here are some thoughts to consider:

- Quantum computing is the next logical evolution from high-performance computing (HPC) in terms of use cases.
- There are hardware approaches -- IBM and Honeywell, for example -- and software approaches -- e.g., Google, AWS -- to quantum computing.
- Vendors have been working with some of their specific centers of excellence and doing extensive investigation out of the CTO office.
- Top vendors leading this initiative are IBM, QCI, Xanadu, Microsoft Azure Quantum and D-Wave Systems.

Although it is still early days for quantum computing, vendors in this area -- such as HPE, Dell and IBM -- are seeing some interesting use cases, and they are exploring them with partners and customers. If they can couple quantum computers with HPC systems, hey believe quantum computers can accelerate certain workloads. In this model, quantum computing can become an accelerator attached to a standard HPC system.

So, who in corporate IT is buying quantum solutions? According to quantum companies, data scientists in education, scientist labs and researchers are the primary users, while common buyers include airline businesses, financial institutions and academia. The conversations focus on the top five applications for initial quantum, which include but are not limited to the following targeted sectors: optimization, research, crypto, finance, materials science and healthcare.

Making moves in the market

Microsoft is making headway with Azure Quantum without a huge investment of hardware. These emulators also have a consortium of companies backing them. QCI, Honeywell, Toshiba, IonQ and iCloud are vendors that discussed their approach, using Azure to achieve their goals.

Google Quantum AI is mostly based on a simulator, but its progress has slowed down since its initial launch in 2019. The Sycamore computer shows potential but is still in its early stage. Amazon Web Services has a quantum computing center focused on R&D, testing and operating quantum processors to innovate and scale tech to support new, large-scale initiatives.

Quantum defines its growth by three horizons:

- **Horizon 1**, also called now or near term, includes transactional use cases such as credit scoring, vehicle routing, chemical design, chemistry and drug/protein structure prediction.
- **Horizon 2**, also called near term, follows with oil processing and shipping, refining processes, drilling, livestock, disruption management and supply chain issues, investment risk analysis, clinical trial acceleration, optimization of manufacturing and fabrication.
- **Horizon 3**, also called future looking, consists of seismic imaging, consumer recommendation with financial analysis, disease risk prediction and structural design for buildings.

Why does any of this matter?

The promise of the quantum computer has been coming for a long time -- and the concept is now becoming a reality. The use of scaling of qubits in real-world environments is showing real potential.

According to Investopedia, "Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory (which explains the behavior of energy and material on the atomic and subatomic levels)." When we look at today's computers, they are designed to encode information in bits that use values of 1 or 0, therefore restricting their ability to achieve this next level of processing. Quantum is a completely new way of computing that differs significantly from what we do today on traditional classical systems.

There are many companies trying to get in front of this "wave" because quantum processing is incredibly fast. Solving today's problems would be completed in a fraction of time. However, not all use cases work with quantum. The traditional systems coexist with quantum systems now and will continue to do so in the future.

32.RSA Conference 2022 Announces Recipients of Lifetime Achievement Award

and Annual Excellence in the Field of Mathematics Award

by Marisa Steck

https://www.rsaconference.com/library/press-release/rsa-conference-2022-announces-recipients-of-lifetime-achievement-award

RSA Conference, the world's leading information security conferences and expositions, today announced the recipients of its 24th annual awards, including the Lifetime Achievement Award and the Award for Excellence in Mathematics. This year, for the first time, the International Association for Cryptologic Research (IACR) co-sponsored the Mathematics Award with RSA Conference.

Established in 1998, the RSA Conference Awards continue to acknowledge the outstanding contributions of individuals and/or organizations whose work helps to continue the fight against cybercrime and help prepare professionals within the industry to perform their jobs at the highest possible level.

"The RSA Conference Awards celebrate inspirational people whose contributions have had a profound, long-lasting effect on the industry and influenced the next generation of industry professionals," said Linda Gray Martin, Vice President, RSA Conference. "These awards are just one way we can recognize their achievements and thank them for their dedication to advancing the field of cybersecurity."

Lifetime Achievement Award

The Lifetime Achievement Award honors outstanding leaders who have made significant contributions to the advancement of the cybersecurity industry over their lifetime. Past recipients represent several of the most influential minds in the field whose work continues to have a lasting impact.

The RSA Conference 2022 Lifetime Achievement Award is posthumously awarded to: **Alan Paller**

Alan founded SANS in 1988, which provides advanced training for 45,000 cybersecurity technologists annually, and was the former president of SANS Technology Institute, the first regionally accredited college focused on educating future cyber stars. Alan served on the board of the National Cyber Scholarship Foundation and led CyberStart, a nationwide on-ramp that allows students to discover and demonstrate cyber talent. He testified before Congress, was a charter member of the President's National Infrastructure Assurance Council, and co-chaired both the DHS Task Force on CyberSkills and the FCC Task Force on Best Practices in Cybersecurity. In 2010, The Washington Post included Alan on its list of "seven people worth knowing in cybersecurity."

Over the years at RSA Conference, Alan led an annual keynote discussion on the most dangerous new attack vectors, to teach companies about what techniques are in use today, what is coming next, and what organizations can do to prepare. During that same session this year titled "The Five Most Dangerous New Attack Techniques," the current president of SANS Technology Institute Ed Skoudis will accept the award on his former colleague's behalf. More information about Alan Paller's legacy can be found here.

"Alan Paller was a beloved colleague and treasured mentor to countless people throughout the cybersecurity community. I can think of no one more deserving of the RSAC Lifetime Achievement Award than the man who dedicated his life to vastly improve cybersecurity practitioners' skills to thwart ever increasing threats," said Ed Skoudis, President of the SANS Technology Institute and Fellow at the SANS Institute. "It is an honor to accept the award on behalf of Alan and his family. Alan was one of the first true visionaries in cybersecurity, with an unmatched passion for educating students. Due to Alan's commitment, hard work and kindness, hundreds of thousands of students have become better cyber defenders. His legacy and lifetime dedication continue to embody the mission of the SANS Institute."

Award for Excellence in the Field of Mathematics, Co-Sponsored by IACR

Each year, RSA Conference recognizes noteworthy work in cryptography and mathematics. Award recipients are determined by an esteemed judging committee who seek to recognize innovation and ongoing contributions to the industry. Dozens of nominated individuals from affiliated organizations, universities or research labs compete each year for this award.

Recipients of the RSA Conference 2022 Excellence in the Field of Mathematics award are:

Professors Cynthia Dwork and Moni Naor

Cynthia Dwork, a professor of Computer Science at the John A. Paulson School of Engineering and Applied Sciences at Harvard University and a Distinguished Scientist at Microsoft Research, is known for establishing the pillars on which every fault-tolerant system has been built atop for decades. Her innovations modernized cryptography to cope with the ungoverned interactions of the internet through the development of non-malleable cryptography, formed the basis of crypto currencies through proofs of work, placed privacy-preserving data analysis on a firm mathematical foundation, and ensures statistical validity in exploratory data analysis, through differential privacy.

"RSA Conference is an important venue for the exchange of ideas in the cybersecurity ecosystem. I am deeply honored to join the ranks of past recipients of this prestigious award that recognizes foundational research," said Dwork. "The threats to privacy have never been greater, and advancements in technology means more cybersecurity risk. My research, work, students, and university will continue to play a key role in helping innovation preserve these values."

Moni Naor is a professor of Computer Science at the Weizmann Institute of Science in Israel specializing in Cryptography and Complexity. He is well known for his work connecting cryptography and data structure in adversarial environments. In 1992, he collaborated with Cynthia Dwork on "Proofs of Work" to combat denial-of-service attacks and other service abuses, such as spam, which is now famous for its use with Bitcoin and blockchain technologies. He has proposed other fundamental concepts that are at the heart of today's cryptography, including non-malleability, broadcast encryption, tracing traitors, small bias probability, and the efficiency of falsifying assumptions.

"The RSA Conference Excellence in the Field of Mathematics Awards has a long list of impressive and impactful recipients dating back to 1998 with Shafi Goldwasser receiving it. I am honored to say that I am now part of the amazing group of cryptographers who have received it," said Naor. "I strongly believe advancements in the field of cryptography will continue to prove necessary as digital communication and usage accelerates. I remain dedicated to making a lasting impact in the field."

"The IACR is proud to join RSAC in co-sponsoring the Excellence in the Field of Mathematics Award. As the worldwide professional society for researchers in cryptography and cryptanalysis, we are dedicated to recognizing individuals who have excelled in our field and advancing awareness of the role cryptology plays in a modern, digitally connected life," said Michel Abdalla, President, IACR. "This year we celebrate the work of Professors Dwork and Naor, and the impact they individually and collectively have had on the cryptography industry and cybersecurity at large."

RSA Conference and IACR presented the Excellence Award in the Field of Mathematics Award on Tuesday, June 7, 2022.

33.SK broadband applies quantum cryptography communication to national convergence network

by Lim Chang-won
https://www.ajudaily.com/view/20220608110410081

SK broadband, a broadband internet service operator in South Korea, has applied quantum cryptography communication technology to a newly established national convergence network as a perfect firewall against eavesdropping or hacking attacks to steal national confidentiality and information.

The application of quantum cryptography communication technology in a network covering a distance of some 800 kilometers (497 miles) would be completed by the end of June. SK broadband said it has developed a technology that connects each section without loss of communication by installing about 30 repeaters.

SK broadband has been selected for a state project to establish a national backbone network that would interconnect individual networks run by 48 government organizations. A backbone network interconnects various other networks in order to create pathways that would allow organizations using a different local area network (LAN) or subnetworks to exchange data.

A dualized backbone network was established for safety, with stability strengthened by making nodes, lines, and equipment double. SK broadband was in charge of the first network centered on cities and provinces. The second mesh network built by LG Uplus (LGU+) connects 21 nodes centered on central government buildings.

SK broadband said some Asian and European countries are trying to benchmark its technology. "This successful application of quantum cryptography technology to an 800 kilometers national convergence network proves that South Korea is the world's best in quantum cryptography technology development and commercialization," Kim Gu-yong, an SK broadband official, said in a statement on June 8.

Cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. SK Telecom (SKT), a top mobile carrier in South Korea, is a leading member of South Korea's state project to secure technology competitiveness in quantum cryptography communication.

SKT's quantum cryptography transmission encryption modules have secured government certification, paving the way for government organizations and public institutions to protect key information against evolving hacking threats by strengthening communication security.

34.Now Is the Time to Plan for Post-Quantum Cryptography

by Karen Spiegelman
https://www.darkreading.com/dr-tech/now-is-the-time-to-plan-for-post-quantum-cryptography

Even the most future-facing panels at this year's RSA Conference are grounded in the lessons of the past. At the post-quantum cryptography keynote "Wells Fargo PQC Program: The Five Ws," the moderator evoked the upheaval from RSAC 1999 when a team from Electronic Frontier Foundation and Distributed.net broke the Data Encryption Standard (DES) in less than a day.

"We're trying to avoid the scramble" when classical cryptography techniques like elliptic curve and the RSA algorithm inevitably fall to quantum decrypting, said Sam Phillips, chief architect for information security architecture at Wells Fargo. And he set up the high stakes encryption battles often have: "Where were all the DES implemented? Hint: ATM machines."

"We had to set up teams to see where all we were using [was DES] and then establish the migration plan based upon using a risk-based approach," Phillips said. "We're trying to avoid that by really trying to get ahead of the game and do some planning in this case."

Phillips was joined on stage by Dale Miller, chief architect of information security architecture at Wells Fargo, and Richard Toohey, technology analyst at Wells Fargo.

A Brief Explanation of Quantum Computing

Toohey, a doctoral candidate at Cornell University, handled most of the technical aspects of quantum computing during the panel.

"For most problems, if you have a quantum calculator and a regular calculator, they can add numbers just as well," he explained. "There's a very small subset of problems that are classically very hard, but for a quantum computer, they can solve [them] very efficiently."

These problems are called NP-hard problems.

"A lot of cryptography, specifically in asymmetric cryptography, relies on these NP-hard type problems — things like elliptic curve cryptography, the RSA algorithm, famously — and when quantum computers are developed enough, they'll be able to brute-force their way through these," Toohey explained. "So that breaks a lot of our modern classical cryptography."

The reason why we don't have crypto-breaking quantum computers today, despite headline-making offerings from IBM and others, is because the technology to reach that level of power has not been accomplished yet.

"To become a cryptographically relevant quantum computer, a quantum computer needs to have about 1 to 10 million logical qubits, and those logical qubits all need to be made up of about 1,000 physical qubits," Toohey said. "Today, right now, the largest quantum computers are somewhere around 120 physical qubits."

He estimated that to even muster the first logical qubit will take three years, and from there it has to scale up to "a million or so logical qubits. So it's still quite a few years away."

Another technical challenge that needs solving before we get these powerful quantum computers is the cooling systems they require.

"Qubits are incredibly sensitive; most of them have to be held at very low, cryogenic temperatures," Toohey explained. "So because of that, quantum computing architecture is incredibly expensive right now."

Other problems include decoherence and error correction. The panel agreed that the combination of these issues means crypto-cracking quantum computers are eight to 10 years away. But that doesn't mean we have a decade to address PQC.

Now Is the Time

The panel was named for the journalistic model of five questions that start with the letter "w," but that didn't come up until late in the audience Q&A portion.

"Sam was asking the what, the who, the why, the where, and the when," Miller said. "So I think we've covered that in our conversations here."

Most of the titular questions were somewhat vague and a matter of judgment. However, on the concept of when you should start planning for the post-quantum future, there was complete agreement: Now.

"You've got to start the process now, and you have to move yourself forward so that you are ready when a quantum computer comes along," Miller said.

Phillips concurred.

"There is not right now a quantum computer that is commercially viable, but the amount of money and effort going into the work is there to move it forward, because people recognize the benefits that are there, and we are recognizing the risk," he said. "We feel that it's an eventuality, that we don't know the exact time, and we don't know when it'll happen."

Toohey suggested beginning preparations with a crypto inventory — again, now.

"Discover where you have instances of certain algorithms or certain types of cryptography, because how many people were using Log4j and had no idea because it was buried so deep?" he said. "That's a big ask, to know every type of cryptography used throughout your business with all your third parties — that's not trivial. That's a lot of work, and that's going to need to be started now."

Wells Fargo has a goal to be ready to run post-quantum cryptography in five uears, which Miller described as "a very aggressive goal."

"So the time to start is now," he said, "and that's one of the most important takeaways from this get-together."

Crypto Agility Gets You to Quantum Resilience

Pivoting is a key marker of agility for the panel, and agility is vital for being able to react to not just quantum threats, but whatever comes next.

"The goal here should be crypto agility, where you're able to modify your algorithms fairly quickly across your enterprise and be able to counter a quantum-based attack," Miller said. "And I'm really not thinking on a day-to-day basis about when is the quantum computer going to get here. For us, it's more about laying a path and a track for quantum resiliency for the organization."

Toomey agreed about the importance of agility.

"Whether it's a quantum computer or new developments in classical computing, we don't want to be put in a position where it takes us 10 years to do any kind of cryptographic transition," he said. "We want to be able to pivot and adapt to the market as new threats come out."

Because there will be computers that can break current cryptography techniques, organizations do need to develop new encryption methods that stand up to quantum brute-force attacks. But that's only the half of it.

"Don't just focus on the algorithms," Phillips said. "Start looking at your data. What data are you transiting back and forth? And look at devaluing that data. Where do you need to have that confidential information, and what can you do to remove that from the exposure? It will help a lot not only in the crypto efforts, but in terms of who has access to the data and why they have to have access."

You've Got to Have Standards

One open question loomed over the discussion: When would NIST announce its picks for the new standards to develop for post-quantum cryptography? The answer: Not yet. But the uncertainty is no cause for inaction, Miller said.

"So NIST will continue to work with other vendors and other companies and research groups to look at algorithms that are further out there," he said. "Our job is to be able to allow those algorithms to come into place quickly, in a very orderly manner, without disrupting business or breaking your business processes and [to] be able to keep things moving along."

Phillips agreed. "That's one of the reasons for pushing on plug and play," he said. "Because we know that the first set of algorithms that come out may not satisfy the long-term need, and we don't want to keep jumping through these hoops every time somebody goes through it."

Toohey tied the standards question back into the concept of preparing now.

"That way, when NIST finally finishes publishing their recommendations, and standards get developed in the coming years, we're ready as an industry to be able to take that and tackle it," he said. "That's going back to crypto agility and this mindset that we need to be able to plug and play. We need to be able to pivot as an industry very quickly to new and developing threats."

35.Faster computing results without fear of errors

by Adam Zewe
https://news.mit.edu/2022/faster-unix-computing-program-0607

Researchers have pioneered a technique that can dramatically accelerate certain types of computer programs automatically, while ensuring program results remain accurate.

Their system boosts the speeds of programs that run in the Unix shell, a ubiquitous programming environment created 50 years ago that is still widely used today. Their method parallelizes these programs, which means that it splits program components into pieces that can be run simultaneously on multiple computer processors.

This enables programs to execute tasks like web indexing, natural language processing, or analyzing data in a fraction of their original runtime.

"There are so many people who use these types of programs, like data scientists, biologists, engineers, and economists. Now they can automatically accelerate their programs without fear that they will get incorrect results," says Nikos Vasilakis, research scientist in the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT.

The system also makes it easy for the programmers who develop tools that data scientists, biologists, engineers, and others use. They don't need to make any special adjustments to their program commands to enable this automatic, error-free parallelization, adds Vasilakis, who chairs a committee of researchers from around the world who have been working on this system for nearly two years.

Vasilakis is senior author of the group's latest research paper, which includes MIT co-author and CSAIL graduate student Tammam Mustafa and will be presented at the USENIX Symposium on Operating Systems Design and Implementation. Co-authors include lead author Konstantinos Kallas, a graduate student at the University of Pennsylvania; Jan Bielak, a student at Warsaw Staszic High School; Dimitris Karnikis, a software engineer at Aarno Labs; Thurston H.Y. Dang, a former MIT postdoc who is now a software engineer at Google; and Michael Greenberg, assistant professor of computer science at the Stevens Institute of Technology.

A decades-old problem

This new system, known as PaSh, focuses on program, or scripts, that run in the Unix shell. A script is a sequence of commands that instructs a computer to perform a calculation. Correct and automatic parallelization of shell scripts is a thorny problem that researchers have grappled with for decades.

The Unix shell remains popular, in part, because it is the only programming environment that enables one script to be composed of functions written in multiple programming languages. Different programming languages are better suited for specific tasks or types of data; if a developer uses the right language, solving a problem can be much easier.

"People also enjoy developing in different programming languages, so composing all these components into a single program is something that happens very frequently," Vasilakis adds.

While the Unix shell enables multilanguage scripts, its flexible and dynamic structure makes these scripts difficult to parallelize using traditional methods.

Parallelizing a program is usually tricky because some parts of the program are dependent on others. This determines the order in which components must run; get the order wrong and the program fails.

When a program is written in a single language, developers have explicit information about its features and the language that helps them determine which components can be parallelized. But those tools don't exist for scripts in the Unix shell. Users can't easily see what is happening inside the components or extract information that would aid in parallelization.

A just-in-time solution

To overcome this problem, PaSh uses a preprocessing step that inserts simple annotations onto program components that it thinks could be parallelizable. Then PaSh attempts to parallelize those parts of the script while the program is running, at the exact moment it reaches each component.

This avoids another problem in shell programming — it is impossible to predict the behavior of a program ahead of time.

By parallelizing program components "just in time," the system avoids this issue. It is able to effectively speed up many more components than traditional methods that try to perform parallelization in advance.

Just-in-time parallelization also ensures the accelerated program still returns accurate results. If PaSh arrives at a program component that cannot be parallelized (perhaps it is dependent on a component that has not run yet), it simply runs the original version and avoids causing an error.

"No matter the performance benefits — if you promise to make something run in a second instead of a year — if there is any chance of returning incorrect results, no one is going to use your method," Vasilakis says.

Users don't need to make any modifications to use PaSh; they can just add the tool to their existing Unix shell and tell their scripts to use it.

Acceleration and accuracy

The researchers tested PaSh on hundreds of scripts, from classical to modern programs, and it did not break a single one. The system was able to run programs six times faster, on average, when compared to unparallelized scripts, and it achieved a maximum speedup of nearly 34 times.

It also boosted the speeds of scripts that other approaches were not able to parallelize.

"Our system is the first that shows this type of fully correct transformation, but there is an indirect benefit, too. The way our system is designed allows other researchers and users in industry to build on top of this work," Vasilakis says.

He is excited to get additional feedback from users and see how they enhance the system. The open-source project joined the Linux Foundation last year, making it widely available for users in industry and academia.

Moving forward, Vasilakis wants to use PaSh to tackle the problem of distribution — dividing a program to run on many computers, rather than many processors within one computer. He is also looking to improve the annotation scheme so it is more user-friendly and can better describe complex program components.

"Unix shell scripts play a key role in data analytics and software engineering tasks. These scripts could run faster by making the diverse programs they invoke utilize the multiple processing units available in modern CPUs. However, the shell's dynamic nature makes it difficult to devise parallel execution plans ahead of time," says Diomidis Spinellis, a professor of software engineering at Athens University of Economics and Business and professor of software analytics at Delft Technical University, who was not involved with this research. "Through just-in-time analysis, PaSh-JIT succeeds in conquering the shell's dynamic complexity and thus reduces script execution times while maintaining the correctness of the corresponding results."

"As a drop-in replacement for an ordinary shell that orchestrates steps, but does not reorder or split them, PaSh provides a no-hassle way to improve the performance of big data-processing jobs," adds Douglas McIlroy, adjunct professor in the Department of Computer Science at Dartmouth College, who previously led the Computing Techniques Research Department at Bell Laboratories (which was the birthplace of the Unix operating system). "Hand optimization to exploit parallelism must be done at a level for which ordinary programming languages (including shells) don't offer clean abstractions. The resulting code intermixes matters of logic and efficiency. It's hard to read and hard to maintain in the face of evolving requirements. PaSh cleverly steps in at this level, preserving the original logic on the surface while achieving efficiency when the program is run."

36.Fastest Supercomputer to Ever Exist Breaks the 'Exascale' Barrier

by Maddie Bender
https://www.vice.com/en/article/4axgym/fastest-supercomputer-to-ever-exist-breaks-the-exascale-barrier

For the first time, a supercomputer has officially broken the exaflop ceiling and become the most powerful computer to ever exist.

The Frontier supercomputer at Oak Ridge National Laboratory was able to demonstrate performance of more than 10^{18} operations per second on a standard test called the TOP500 that ranks the 500 most powerful commercially available computer systems, according to the organization.

High expectations were set for Frontier in 2019, when its construction was first announced. Now, three years later, it is in its final testing phases with plans to fully open in early 2023.

"Science today is driven by simulation," said Jack Dongarra, a distinguished professor of computer science at the University of Tennessee who helps lead the TOP500. "Simulation is done on supercomputers, and it's often said that the fastest supercomputer can drive the best science."

One of the biggest challenges to designing an exascale supercomputer like Frontier was figuring out how to lower energy costs. Initially, researchers predicted these machines might use the same amount of energy as 50 homes; working with vendors to lower the amount of energy required got the computer's power down to roughly 20 megawatts per exaflop, or under a tenth of early estimates.

This milestone for Frontier makes strides toward fulfilling the Department of Energy's 2018 promise to build a trio of exascale computers at Oak Ridge, Argonne, and Livermore National Laboratories, budgeting up to $1.8 million for the entire project. These computers will enable modeling and forecasting at precisions never before seen that will drive innovation forward in medicine, engineering, and nuclear energy, Dongarra said; exascale technology can even improve financial risk modeling and animation, he added.

These incredibly powerful systems will eventually be complemented by quantum computers, which are better than these traditional supercomputers at solving certain types of problems (for instance, those relating to cryptography.) In the future, Dongarra said he could foresee integrating components that drive traditional supercomputing and quantum computing to power a computer that can quickly solve both types of problems.

When Frontier is up and running, it will function like a crystal ball for modelers and forecasters, Dongarra said. Still, it's nowhere near the final destination for supercomputing.

“This is not the end of the story,” he said. “It's the continuation of a road where we will build bigger and faster supercomputers to help us solve some of the most challenging problems that we have today.”

37.Developing the next generation of quantum algorithms and materials

by Sarah Wong
https://phys.org/news/2022-06-quantum-algorithms-materials.html

Quantum computers are expected to revolutionize the way researchers solve difficult computing problems. These computers are being designed to tackle major challenges in fundamental research areas, such as quantum chemistry. In its current stage of development, quantum computing is still very sensitive to noise and disruptive factors in the environment. This makes quantum computing "noisy" as quantum bits—or qubits—lose information by getting out of sync, a process called decoherence. To overcome the limitations of current quantum computers, researchers at Pacific Northwest National Laboratory (PNNL) are developing simulations that provide a glimpse into how quantum computers work.

"When we try to directly observe the behavior of quantum systems, like qubits, their quantum states will collapse," said PNNL Computer Scientist Ang Li. Li is also a researcher for the Quantum Science Center and the Co-Design Center for Quantum Advantage—two of the five Department of Energy National Quantum Information Science Research Centers. "To get around this, we use simulations to study qubits and their interaction with the environment.”

Li and collaborators at Oak Ridge National Laboratory and Microsoft use high performance computing to develop simulators that mimic real quantum devices for executing complex quantum circuits. Recently, they combined two different types of simulations to create the Northwest Quantum Simulator (NWQ-Sim) to test quantum algorithms.

"Testing quantum algorithms on quantum devices is slow and costly. Also, some algorithms are too advanced for current quantum devices," said Li. "Our quantum simulators can help us look beyond the limitations of existing devices and test algorithms for more sophisticated systems."

Algorithms for quantum computers

Nathan Wiebe, a PNNL joint appointee from the University of Toronto and affiliate professor at the University of Washington, is taking another strategy with writing code for quantum computers. Though it can be frustrating at times to be limited by the capabilities of current quantum devices, Wiebe sees this challenge as an opportunity.

"Noisy quantum circuits produce errors in calculations," said Wiebe. "The more qubits that are needed for a calculation, the more error-prone it is."

Wiebe and collaborators from the University of Washington developed novel algorithms to correct for these errors in certain types of simulations.

"This work provides a cheaper and faster way to perform quantum error correction. It potentially brings us closer to demonstrating a computationally useful example of a quantum simulation for quantum field theory on near-term quantum hardware," said Wiebe.

Dark matter meets quantum computing

While Wiebe seeks to mitigate noise by creating algorithms for error correction, Physicist Ben Loer and his colleagues look to the environment to control external sources of noise.

Loer uses his background in achieving ultra-low levels of natural radioactivity—required to search for experimental evidence of dark matter in the universe—to help prevent qubit decoherence.

"Radiation from the environment, such as gamma rays and X-rays, exists everywhere," said Loer. "Since qubits are so sensitive, we had an idea that this radiation may be interfering with their quantum states."

To test this, Loer, project lead Brent VanDevender, and colleague John Orrell, teamed up with researchers at the Massachusetts Institute of Technology (MIT) and MIT's Lincoln Laboratory used a lead shield to protect qubits from radiation. They designed the shield for use within a dilution refrigerator—a technology used to produce the just-above-absolute-zero temperature necessary for operating superconducting qubits. They saw that qubit decoherence decreased when the qubits were protected.

While this is the first step towards understanding how radiation affects quantum computing, Loer plans to look at how radiation disturbs circuits and substrates within a quantum system. "We can simulate and model these quantum interactions to help improve the design of quantum devices," said Loer.

Loer is taking his lead-shielded dilution refrigerator research underground in PNNL's Shallow Underground Laboratory with the help of PNNL Chemist Marvin Warner

"If we develop a quantum device that doesn't perform as it should, we need to be able to pinpoint the problem," said Warner. "By shielding qubits from external radiation, we can start to characterize other potential sources of noise in the device."

38.Tech policy groups push back against India's new cybersecurity rules

by Aashish Aryan & Dia Rekhi

https://economictimes.indiatimes.com/tech/technology/cert-ins-directives-on-reporting-cybersecurity-incident-lacks-clarity-software-policy-group-bsa/articleshow/92021261.cms?from=mdr

The directive of the Indian Computer Emergency Response Team (Cert-In) on reporting a cybersecurity incident within six hours from being aware of it and the lack of clarity on what constitutes a severe or a large-scale incident among other things could potentially "undermine incident investigation and response, including the deployment of defensive measures", software policy group BSA has said.

"We recommend that the directions ask to provide an initial report of high-impact or severe cyber incidents as soon as practicable or within 72 hours of the confirmation of an incident, whichever is faster," Venkatesh Krishnamoorthy, country manager India at BSA, the Software Alliance, said in a letter to the Ministry of Electronics and Information Technology on May 30.

Several other **tech policy** and business advocacy organisations have also raised concerns over Cert-In's directives. The US India Business Council, the Cybersecurity Coalition, US Chamber of Commerce, the Bank Policy Institute, the Internet and Mobile Association of India, AccessNow and SFLC.in have written to the ministry and Cert-In, claiming that rules such as retaining customer details for five years by virtual private network (VPN) providers would "put people's privacy at risk".

"They expand the scope of mass surveillance, contravene globally recognised principles of necessity and proportionality, and data minimisation, and ultimately weaken cybersecurity. They effectively create new cybersecurity vulnerabilities in the form of databases of retained data that can be exploited by malicious actors," AccessNow had said in a June 1 letter to Cert-In.

On April 28, Cert-In had come out with a set of guidelines for all companies, intermediaries, data centres and government organisations under which any data breach must be reported to the government within six hours of the organisation becoming aware of it.

These guidelines had also mandated that VPN service providers shall maintain all the information they had gathered as a part of know-your-customer rules and hand it over to the government as and when asked for it.

On May 18, the Ministry of Electronics and Information Technology came out with a set of frequently asked questions on the Cert-In guidelines during which it clarified certain aspects of how the sixhour norm would work, along with what details the VPN service providers would have to keep for five years.

Indicating the government's tough stand on the issue, minister of state for information technology Rajeev Chandrasekhar had said VPN service providers which did not want to adhere to the latest cybersecurity guidelines were "free to leave India".

39.Quantum machine Borealis achieves computational advantage using programmable photonic sensor

by Bob Yirka
https://phys.org/news/2022-06-quantum-machine-borealis-advantage-programmable.html

A team of researchers from Xanadu in Canada and the National Institutes of Standards and Technology, in the U.S., is claiming that their quantum computer, Borealis, has achieved computational advantage in taking on the boson sampling challenge. In their paper published in the journal Nature, the group describes their computer and how well it performed when tackling the challenge. Daniel Jost Brod, with the Federal Fluminense University, in Brazil, has published a News & Views piece in the same journal issue outlining the short history of quantum computing and the work done by the team on this new effort.

As work continues toward a truly usable quantum computing machine, research groups add more power to the devices they are working on and then subject them to computational advantage tests. Such tests are meant to show that a given device is able to process a problem that would take conventional computers so long to run that doing so would be impractical.

In this new effort, the researchers took on the boson sampling challenge using a photonic machine that uses photons to represent qubits. Technically called the Gaussian boson sampling challenge, it involves preparing states of light and directing them through a network of beam splitters and then counting how many of the photons arrive at a detector. The best modern computers get bogged down quickly when attempting the challenge, whereas theory has suggested a quantum computer should shine. Prior efforts to take on the challenge have involved the use of 76 to 113 photons. The machine built by the team on this new effort was able to access up to 219 photons, while it averaged 125—a significant leap forward.

In running the challenge, the team found that Borealis was able to perform the specified task in 36 microseconds. The researchers calculated that it would have taken the best traditional computer approximately 9,000 years to accomplish the same task. This difference, the researchers claim, shows computational advantage. The researchers took their work one step further by testing the output given by Borealis and showed that it could not be spoofed, evidence that the answers it gave were correct.

40.What's So Great About Quantum Computing? A Q&A With NIST Theorist Alexey Gorshkov

by NIST
https://www.nist.gov/blogs/taking-measure/whats-so-great-about-quantum-computing-qa-nist-theorist-alexey-gorshkov

As the rise of quantum computers becomes the subject of more and more news articles — especially those that prophesy these devices' ability to crack the encryption that protects secure messages, such as our bank transfers — it's illuminating to speak with one of the quantum experts who is actually developing the ideas behind these as-yet-unrealized machines. Whereas ordinary computers work with bits of data that can be either 0 or 1, quantum computers work with bits — called qubits — that can be 0 and 1 simultaneously, enabling them to perform certain functions exponentially faster, such as trying out the different "keys" that can break encryption.

Simple quantum computers already exist, but it has been extremely challenging to build powerful versions of them. That's because the quantum world is so delicate; the tiniest disturbances from the outside world, such as stray electrical signals, can cause a quantum computer to crash before it can carry out useful calculations.

NIST public affairs specialist Chad Boutin interviewed Alexey Gorshkov, a NIST theorist at NIST/University of Maryland's Joint Center for Quantum Information and Computer Science (QuICS) and Joint Quantum Institute, who works at the intersection of physics and computer science research. His efforts are helping in the design of quantum computers, revealing what capabilities they might possess, and showing why we all should be excited about their creation.

We all hear about quantum computers and how many research groups around the world are trying to help build them. What has your theoretical work helped clarify about what they can do and how?

I work on ideas for quantum computer hardware. Quantum computers will be different from the classical computers we all know, and they will use memory units called qubits. One thing I do is propose ideas for various qubit systems made up of different materials, such as neutral atoms. I also talk about how to make logic gates, and how to connect qubits into a big computer.

Another thing my group does is propose quantum algorithms: software that one can potentially run on a quantum computer. We also study large quantum systems and figure out which ones have promise for doing useful computations faster than is possible with classical computers. So, our work covers a lot of ground, but there's a lot to do. You have this big, complicated beast in front of you and you're trying to chip away at it with whatever tools you have.

You focus on quantum systems. What are they?

I usually start by saying, at very small scales the world obeys quantum mechanics. People know about atoms and electrons, which are small quantum systems. Compared to the big objects we know, they are peculiar because they can be in two seemingly incompatible states at once, such as particles being in two places at the same time. The way these systems work is weird at first, but you get to know them.

Large systems, made up of a bunch of atoms, are different from individual particles. Those weird quantum effects we want to harness are hard to maintain in bigger systems. Let's say you have one atom that's working as a quantum memory bit. A small disturbance like a nearby magnetic field has a chance of causing the atom to lose its information. But if you have 500 atoms working together, that disturbance is 500 times as likely to cause a problem. That's why classical physics worked well enough for so many years: Because classical effects overwhelm weird quantum effects so easily, usually classical physics is enough for us to understand the big objects we know from our everyday life.

What we're doing is trying to understand and build large quantum systems that "stay quantum" — something we specialists call "coherent" — even when they are large. We want to combine lots of ingredients, say 300 qubits, and yet ensure that the environment doesn't mess up the quantum effects we want to harness. Large coherent systems that are not killed by the environment are hard to create or even simulate on a classical computer, but coherence is also what will make the large systems powerful as quantum computers.

What is compelling about a large quantum system?

One of the first motivations for trying to understand large quantum systems is potential technological applications. So far quantum computers haven't done anything useful, but people think they will very soon and it's very interesting. A quantum internet would be a secure internet, and it also would allow you to connect many quantum computers to make them more powerful. I'm fascinated by these possibilities.

It's also fascinating because of fundamental physics. You try to understand why this system does some funny stuff. I think a lot of scientists just enjoy doing that.

Why are you personally so interested in quantum research?

I got my first exposure to it after my junior year in college. I quickly found it has a great mix of math, physics, computer science and interactions with experimentalists. The intersection of all these fields is why it's so much fun. I like seeing the connections. You end up pulling an idea from one field and applying it to another and it becomes this beautiful thing.

Lots of people worry that a quantum computer will be able to break all our en-

cryption, revealing all our digitized secrets. What are some less worrying things they might be able to do that excite you?

Before I get into what excites me, let me say first that it's important to remember that not all of our encryption will break. Some encryption protocols are based on math problems that will be vulnerable to a quantum computer, but other protocols aren't. NIST's post-quantum cryptography project is working on encryption algorithms that could foil a quantum computer.

As for what excites me, lots does! But here are a couple of examples.

One thing we can do is simulation. We might be able to simulate really complicated things in chemistry, materials science and nuclear physics. If you have a big complex chemical reaction and you want to figure out how it's taking place, you have to be able to simulate a big molecule that has lots of electrons in a cloud around it. It's a mess, and it's hard to study. A quantum computer can in principle answer these questions. So maybe you could use it to find a new drug.

Another possibility is finding better solutions to what are called classical optimization problems, which give classical computers a lot of trouble. An example is, "What are more efficient ways to direct shipments in a complex supply chain network?" It's not clear whether quantum computers will be able to answer this question any better than classical computers, but there's hope.

A follow-up to the previous question: If quantum computers aren't actually built yet, how do we know anything about their abilities?

We know — or think we know — the microscopic quantum theory that qubits rely on, so if you put these qubits together, we can describe their capabilities mathematically, and that would tell us what quantum computers might be able to do. It's a combination of math, physics and computer science. You just use the equations and go to town.

There are skeptics who say that there might be effects we don't know about yet that would destroy the ability of large systems to remain coherent. It's unlikely that these skeptics are right, but the way to disprove them is to run experiments on larger and larger quantum systems.

Are you chasing a particular research goal? Any dreams you'd like to realize someday, and why?

The main motivation is a quantum computer that does something useful. We're living in an exciting time. But another motivation is just having fun. As a kid in eighth grade, I would try to solve math problems for fun. I just couldn't stop working on them. And as you have fun, you discover things. The types of problems we are solving now are just as fun and exciting to me.

Lastly, why NIST? Why is working at a measurement lab on this research so important?

Quantum is at the heart of NIST, and its people are why. We have top experimentalists here including multiple Nobel laureates. NIST gives us the resources to do great science. And it's good to work for a public institution, where you can serve society.

In many ways, quantum computing came out of NIST and measurement: It came out of trying to build better clocks. Dave Wineland's work with ions is important here. Jun Ye's work with neutral atoms is too. Their work led to the development of amazing control over ions and neutral atoms, and this is very important for quantum computing.

Measurement is at the heart of quantum computing. An exciting open question that lots of people are working on is how to measure the "quantum advantage," as we call it. Suppose someone says, "Here is a quantum computer, but just how big is its advantage over a classical computer?" We're proposing how to measure that.

41.Advanced quantum computer made available to the public for first time

by Alex Wilkins
https://www.newscientist.com/article/2322807-advanced-quantum-computer-made-available-to-the-public-for-first-time/

A quantum computer that encodes information in pulses of light has solved a task in 36 microseconds that would take the best supercomputer at least 9000 years to complete. The researchers behind the machine have also connected it to the internet, allowing others to program it for their own use – the first time such a powerful quantum computer has been made available to the public.

Quantum computers rely on the strange properties of quantum mechanics to theoretically perform certain calculations far more quickly than conventional computers. A long-standing goal in the field, known as quantum advantage or quantum supremacy, has been to demonstrate that quantum computers can actually beat regular machines. Google was the first to do so in 2019 with its Sycamore processor, which can solve a problem involving sampling random numbers that is essentially impossible for classical machines.

Now, Jonathan Lavoie at Xanadu Quantum Technologies in Toronto, Canada, and his colleagues have built a quantum computer called Borealis that uses particles of light, or photons, travelling through a series of fibre-optic loops to solve a problem known as boson sampling. This involves measuring the properties of a large group of entangled, or quantum-linked, photons that have been separated by beam splitters.

Boson sampling is a difficult task for ordinary computers because the complexity of the calculations drastically rises as the number of photons increases. Borealis essentially computes the answer by directly measuring the behaviour of up to 216 entangled photons.

Solving this problem isn't particularly useful outside of establishing that quantum advantage has been achieved, but it is an important test. "By demonstrating these results using Borealis, we have validated key technologies that we need for the quantum computers of the future," says Lavoie.

Borealis is the second device to demonstrate quantum advantage in boson sampling. The first is a machine called Jiuzhang, created by researchers at the University of Science and Technology of China (USTC). It first showed quantum advantage in 2020 with 76 photons and then again in an improved version in 2021 using 113 photons. The USTC team also demonstrated quantum advantage last year in the random-number-sampling problem, with a machine called Zuchongzhi.

More power

Borealis is an advance on Jiuzhang because it is a more powerful system, capable of calculating with a larger number of photons, and has a simplified architecture, says Peter Knight at Imperial College London. "We all thought that the Chinese experiment was a tour de force, but we couldn't see that it was going to go any further because there was a limit to how much stuff you could cram onto your optical table," he says.

Compared with Borealis, Jiuzhang uses a larger number of beam splitters to send entangled photons in lots of different directions. But Borealis takes a different approach, using loops of optical fibre to delay the passage of some photons relative to others – separating them in time, rather than space.

An added benefit of the stripped-back design is that this computer is more easily controllable, so it can also be reprogrammed remotely for people to run it with their own settings. "Borealis is the first machine capable of quantum computational advantage made publicly available to anyone with an internet connection," says Lavoie.

People will probably begin by testing variations of boson sampling, says Knight, but, later on, it may be possible to apply Borealis to different problems. So far, no one has been able to demonstrate quantum advantage for a "useful" computational task – the random-sampling problem first tackled by Google essentially has no applications beyond demonstrating quantum advantage.

While Borealis is an impressive jump forward in scale over Jiuzhang, it falls short of being a fully programmable quantum computer like Sycamore or Zuchongzhi, says Raj Patel at the University of Oxford. This is because a component called an interferometer, which measures interference patterns to extract information from the photons, has been limited to only record certain photon interactions in an effort to get clearer readings. "To create a machine that is programmable and can tackle real-world problems, you would really want the interferometer to be fully connected," says Patel.

Lavoie and his colleagues are now working to turn a blueprint they released last year into a scalable, fault-tolerant photonic processor built on an integrated chip, which would improve the quantum machine's capabilities even further.

42.Receiver-Device-Independent Quantum

Key Distribution (QKD)

by Karine

https://thequantumhubs.com/receiver-device-independent-quantum-key-distribution-qkd/

Researchers at University of Geneva (UNIGE) and CEA have presented new protocols for Quantum Key Distribution (QKD) in a prepare-and-measure setup with an asymmetric level of trust.

While the device of the sender (Alice) is partially characterized, the receiver's (Bob's) device is treated as a black-box. The security of the protocols is based on the assumption that Alice's prepared states have limited overlaps, but no explicit bound on the Hilbert space dimension is required. The protocols are immune to attacks on the receiver's device, such as blinding attacks.

The users can hence establish a secret key while continuously monitoring the correct functioning of their devices through observed statistics.

The team reported a proof-of-principle demonstration, involving mostly off-the-shelf equipment, as well as a high-efficiency superconducting nanowire detector. A positive key rate is demonstrated over a 4.8 km low-loss optical fiber with finite-key analysis.