Crypto News

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

September 01, 2022

Table of Contents

Editorial

Is it September already? Seems so and it's time for our next issue of Crypto News! Do you work in critical infrastructure and are struggling with how to prepare for post quantum cryptography? Head over the article #5. The Cybersecurity and Infrastructure Agency (CISA) in the USA has released information and documentation after conducting an assessment on quantum vulnerabilities to National Critical Functions (NCFs). Besides a CISA Insight document outlining how to prepare, there is also a post-quantum cryptography roadmap that can be found on their websites. Links to both are in the article.

Now picture this … a future where there is no counterfeit cash using, you guessed it, quantum cryptography. As economists and the Notorious B.I.G. have said for years, "mo' money (necessarily correlates with) mo' problems." In an effort to provide a solution for at least one of the money related problems for the US government, researchers at MIT and Harvard have theorized that in the future quantum cash may save the US economy $30 billion - $50 billion annually. How would this be done? The researchers state that "a successful quantum money protocol would require three features; the efficient creation of money states, the efficient public authentication, and unforgeability." Want to learn more? Head over to article #15 for all of the details. Happy reading!

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

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

1.Crypto Quantique's quantum-driven silicon IP enables root-of-trust in the Intel Path-finder for RISC-V environment

https://www.design-reuse.com/news/52565/crypto-quantique-quantum-driven-silicon-ip-root-of-trust-intel-pathfinder-risc-v.html

Crypto Quantique, a specialist in quantum-driven cyber security for the internet of things (IoT), announces that the company's QDID silicon IP block has been selected for the recently announced Intel® Pathfinder for RISC-V* integrated development environment. Intel® Pathfinder enables RISC-V cores and other IP to be evaluated in FPGAs and simulator programs before committing to the final silicon design and fabrication. The environment is supported by industry-standard toolchains.

QDID is the first security IP chosen for Intel Pathfinder. QDID is independently verified as resilient against all currently-known cyberattack mechanisms. Its analog block measures random, quantum tunnelling current in the fabric of silicon wafers to produce high-entropy, random numbers from which unique, unforgeable identities and cryptographic keys are created on-demand. These identities and keys form a root-of-trust for each device, and this is the foundation for IoT security when QDID chips are deployed.

Because QDID's random numbers are generated within the fabric of the silicon, both key injection and the need to store cryptographic keys in memory are eliminated. This gives semiconductor users total control of their security framework and enables them to create in a zero-trust supply chain that eliminates several security vulnerabilities.

QDID is complemented by Crypto Quantique's QuarkLink end-to-end IoT security software. The QuarkLink platform enables thousands of end point devices to be connected to on-premises or cloud servers automatically through cryptographic APIs. Via a simple graphical user interface, users can achieve secure provisioning, onboarding, security monitoring, and certificate and key renewal or revocation with just a few keystrokes.

Crypto Quantique's CEO, Dr. Shahram Mossayebi, said, "QDID for Intel® Pathfinder RISC-V* is further validation of our technology leadership in IoT security. QDID is easily integrated into the security framework of the RISC-V architecture and, just as Intel is helping democratize chip design with its Intel Pathfinder development environment, QDID and QuarkLink are democratizing semiconductor security by making it technically and economically accessible for the broadest possible range of applications."

"The integration of Crypto Quantique with Intel® Pathfinder demonstrates our commitment to addressing key end-user concerns like security at an early stage in the development process," said Vijay Krishnan, General Manager, RISC-V Ventures from Intel, "thus paving the way for increased RISC-V adoption in segments like IoT."

2.Unlocking the secret to private messaging apps

by CECILIA DUONG
https://newsroom.unsw.edu.au/news/science-tech/unlocking-secret-private-messaging-apps?utm_source=linkedin&utm_medium=social

Whether you're sharing confidential information or swapping movie ideas with a friend, people are turning to

private messaging apps that offer end-to-end encryption to protect the contents of their conversations.

When data is shared over the internet, it often traverses a series of networks to reach its destination. Apps such as WhatsApp, owned by social media giant Meta (formerly Facebook), provide a level of privacy that even challenges Government agencies from accessing encrypted conversations.

However, with the apps constantly changing their security and privacy policies, are the messages still safe from being decrypted?

Back in May 2021, disapproval by the online community with the changes to WhatsApp's privacy policy for business entities using the platform, saw many users switch to other private messaging apps such as Signal and Telegram.

Cybersecurity expert, Dr Arash Shaghaghi from UNSW School of Computer Science and Engineering and UNSW Institute for Cyber Security, compares encryption to the likes of having a secret conversation between you and another person.

"To keep our information away from prying eyes, we rely on cryptographic algorithms to encrypt our data. Encryption involves converting human-readable plaintext into an encoded format and the data can only be read after it's been decrypted," he says.

"Encryption involves using a key to lock a message, while decryption is using a key to unlock a message.

"In theory, if an outsider observed an encrypted conversation, they could not make sense of it, and they will need the appropriate key to decrypt it.

"Interestingly, with some end-to-end encryption protocols, such as Signal, even if someone steals the encryption keys and taps over the connection, they cannot decrypt messages already sent. In crypto parlance, this is termed as forward secrecy."

Are our messages fully secure?

Modern encryption algorithms have been battle-tested and shown to have no known vulnerabilities. While it doesn't mean it's impossible to crack, the process requires extensive processing powers and could take a significantly long time to do. Quantum computers, if they mature enough, will be able to crack much of today's encryption.

Attackers commonly target endpoints and their vulnerabilities. This is much easier than cryptanalysis which is the process used to breach cryptographic security systems.

For instance, last year, attackers targeted a vulnerability related to WhatsApp's image filter functionality that was triggered when a user opened an attachment containing a maliciously crafted image file. There have been more serious and less complicated vulnerabilities reported targeting WhatsApp clients running on iOS and Android.

Dr Shaghaghi says when you back up your messages on some of the messaging platforms, your messages are pushed to the cloud. This means that all your messages are now stored on someone else's computer.

"The service provider's implementation of end-to-end encryption plays a significant role in the security and privacy of a messaging app against the provider and attackers," he says.

"WhatsApp used to keep a backup of the messages in an unencrypted format over iCloud for Apple users and Google Drive for those who used WhatsApp in Android. Even though WhatsApp adopted an end-to-end encryption model in 2016, unencrypted backups were vulnerable to government requests, third-party hacking, and disclosure by Apple or Google employees."

In 2021, WhatsApp rolled out an option for users to enable end-to-end encryption of their backups. While this was welcomed as a positive step forward, it should be the default for all users - not offered as an option, says Dr Shaghaghi.

“Users concerned about the security and privacy of their data must make sure to enable the end-to-end encryption backup for WhatsApp and other messaging platforms”.

What about Signal and Telegram?

Unlike WhatsApp and Signal, Telegram does not have end-to-end encryption enabled by default. Only when the ‘secure chat’ function is enabled, Telegram applies the MTProto protocol, an open-source and custom-developed protocol by the messaging provider.

“As far as we know, Signal, Telegram and WhatsApp are secure in providing end-to-end encryption, if the option is enabled,” says Dr Shaghaghi.

“However, Signal is built with privacy and security as the primary motivation. Signals’ endpoint source code is also available to the public – this allows anyone to inspect the code and identify vulnerabilities.

“I believe the consensus is that Signal is a more secure and privacy-friendly messaging solution when compared to WhatsApp, Telegram, or Facebook Messenger.”

With so many messaging platforms available on the market, Dr Shaghaghi says there are some simple steps to take to help safeguard a user’s privacy.

“Messaging platforms contain a lot of private information so it's worth ensuring that the platform we use has a good reputation for ensuring the security and privacy of its users,” he says.

“It is also worth spending a few extra minutes to enable some of the more advanced security features these platforms offer, such as end-to-end backup encryption or multi-factor authentication.

“And whichever platform you decide to use, it’s best practice to ensure we use the latest version of the apps and avoid downloading apps from third-party stores.”

Moderating content exchanged over end-to-end encrypted messaging platforms

There have been strong calls by different Government organisations for these apps to include backdoors which would provide access to data when deemed required by authorities.

Recent leaks from the US Federal Bureau of Investigation (FBI) demonstrated that even with a subpoena, powerful government entities have limited access to messages exchanged over apps that use end-to-end encryption.

This argument is especially worrying for many users who are concerned that it’s the first step away from the strong encryption principles that they rely on to ensure the security and privacy of their data.

There have been ongoing debates in Australia and overseas regarding this topic.

“From a security engineering perspective, implementing a backdoor is never a good idea”, says Dr Shaghaghi.

“There is no guarantee that malicious hackers do not find out about these backdoors too and exploit them.

“However, those in favour of a solution allowing access for law enforcement agencies argue that they need access given the increasing usage of these platforms by criminals.”

Some messaging providers and tech companies have responded by making changes to the functionality of the platform.

“To meet regulatory requirements, WhatsApp now allows users to flag a message to be reviewed by their moderators. This needs to be initiated by a user and when a message is flagged, the few messages before it is also forwarded to WhatsApp moderators,” says Dr Shaghaghi.

"Apple has promoted encrypted messaging across its ecosystem and have fought off law enforcement agencies looking for records.

“In 2021, they announced child safety features that include detecting sexually explicit pictures over iMessage, another platform using end-to-end encryption. To implement this feature, Apple plans to implement the detection on the device and not through an encryption backdoor.

“I think we can balance the need for moderating criminal content and security and privacy requirements by breaking down the problem into more specific use-cases and developing innovative solutions.”

3.Action required now to prepare for quantum computing cyber threats

by Danny Palmer
https://www.zdnet.com/article/quantum-computing-poses-cyber-threats-to-critical-infrastructure-action-to-secure-it-is-needed-now-warns-cisa/

Action must be taken now to help protect networks from cybersecurity threats that will emerge in the advent of power of quantum computing, the US Cybersecurity and Infrastructure Security Agency (CISA) has warned.

While quantum computing could bring benefits to computing and society, it also brings new cybersecurity threats – and the CISA alert warns that critical infrastructure in particular is at risk.

Many forms of digital communications and internet-connected systems rely on data encryption to protect them from cyber attackers. Public key cryptography helps to protect information from being viewed by unauthorised intruders – and it's extremely difficult to crack using today's computers.

But quantum computing will bring much higher levels of computing power and speed, capable of breaking public key cryptography and threatening cybersecurity in a wide range of areas including online banking, secure communications and digital signatures.

Researchers have warned that the cybersecurity of infrastructure that supports critical national services – including electricity, fuel, water and transport – could be at significant risk.

Much of this is due to the dependence on industrial control systems (ICSs), which have long life cycles and rarely receive updates. This means that critical infrastructure providers who aren't prepared could be left vulnerable to attacks.

It's therefore recommended that critical infrastructure providers make the necessary preparations to mitigate post-quantum cryptography now, rather than waiting for the technology to become more widespread.

"CISA urges ICS organizations to ensure that their hardware replacement cycles, and cybersecurity risk management strategies account for actions to address risks from quantum computing capabilities," said the alert.

"Do not wait until the quantum computers are in use by our adversaries to act. Early preparations will ensure a smooth migration to the post-quantum cryptography standard once it is available."

While the expense and expertise required to develop quantum computing technology are currently restricted to large technology companies, research institutions or nation-states, as it becomes more widely available, it could become a major cybersecurity issue for everyone.

"In the hands of adversaries, sophisticated quantum computers could threaten U.S. national security if we do not begin to prepare now for the new post-quantum cryptographic standard," warned CISA.

CISA has previously set out a post-quantum cryptography roadmap to help organisations protect their data and systems and to reduce risks related to the advancement of quantum computing technology.

4.Free Quantum Computing Training Course Launched by the Linux Foundation & World Bank

by JAMES DARGAN
https://thequantuminsider.com/2022/08/26/free-quantum-computing-training-course-launched-by-the-linux-foundation-world-bank/?utm_source=newsletter&utm_medium=email&utm_term=2022-08-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Ee-roQ+Sails+Brand+New+Q+From+Baidu+And+More+Quantum+News

The Linux Foundation, the nonprofit organization enabling mass innovation through open source, has released a new, free, online training course, Fundamentals of Quantum Computing, in partnership with the World Bank. The course provides an understanding of how quantum computing could be used for complex decision-making far beyond current computer capabilities, as well as an understanding of the technological, governmental, and industrial implications as the technology further matures.

Quantum computing involves using quantum theories to perform complex computations. The technology has been in development for decades and is expected to revolutionize computing as it becomes more widely available.

The Linux Foundation has been providing access to online training and education since 2014 and offers a full course catalog across a dozen categories with 100+ course offerings to meet a growing demand around the world. At the same time, the World Bank Group's Open Learning Campus (OLC) serves to accelerate development solutions by transforming global knowledge into actionable learning. Since its inception in 2015, it has provided 5000 learning offerings to over 4 million clients in 190 countries. This helps to meet the World Bank Group's twin goals of ending poverty and building shared prosperity.

"Quantum computing has the potential to impact various sectors, including financial services, healthcare, agriculture and logistics, in addition to changing the way we architect cybersecurity. Given its potential impact, it is important to develop foundational knowledge of this new technology as it develops, to understand its implications for our skills, systems and technological governance," said Sheila Jagannathan, head of the Open Learning Campus at the World Bank. "As part of the Bank Group's ongoing efforts to support Government Chief Information Officers, government technology teams, advisors, and policymakers considering and preparing for the practical aspects of digital transformation in emerging economies, we have worked with Linux Foundation to develop this course on Quantum Computing fundamentals. This is part of a broader initiative to learn from our advanced digital partners, including the Republic of Korea, on the current and future impact of emerging technologies."

The new course takes approximately three hours to complete, making it accessible to anyone. It will be of particular interest for public sector leaders, Chief Information Officers (CIOs), and technology teams in charge of the planning, design, development and deployment of public service delivery and digital economy infrastructures and platforms. Learners should be generally familiar with how computers function and the current use of on-premise and cloud computing.

The course discusses the fundamentals of quantum computing, highlighting potential technological disruptions it brings. It discusses the current capabilities of quantum computing, current use cases, as well as prospective future applications, while emphasizing security advantages and dangers, especially around secure communication and encryption. It also dispels some of the myths surrounding quantum computing, explaining what it is at the moment, as well as why it is an exciting and essential technology to understand and embrace.

"We are on the cusp of another technological revolution as quantum computing technology matures and enables us to solve problems which are too computationally intensive for traditional computers," said Clyde Seepersad, SVP, and general manager of training & certification at the Linux Foundation. "Now is the time to start teaching folks around the world about quantum computing in order to ensure that the policy implications are thought through and that the requisite talent pool is nurtured to support this technology as it grows. The World Bank has proven to be a valuable partner in this endeavor, recognizing the need and taking a leadership role in ensuring educational resources are available around quantum computing to everyone."

Fundamentals of Quantum Computing is available for immediate, free registration. The course can be accessed both on the World Bank Group's OLC and the Linux Foundation Training Platform.

5.CISA Releases Guidelines to Aid Companies Transition to Post-quantum Cryptography

by Alessandro Mascellino
https://www.infosecurity-magazine.com/news/cisa-transition-post-quantum/

The Cybersecurity and Infrastructure Security Agency (CISA) has released an Insight document named 'Preparing Critical Infrastructure for Post-Quantum Cryptography.'

The resource aims to provide an overview of the potential impacts of quantum computing on National Critical Functions (NCFs), alongside recommended actions critical infrastructure and government network owners and operators should take to prepare for the transition.

"While post-quantum computing is expected to produce significant benefits, we must take action now to manage potential risks, including the ability to break public key encryption that U.S. networks rely on to secure sensitive information," explained Mona Harrington, acting assistant director of national risk management center at CISA.

The CISA Insight is reportedly based on findings from an assessment conducted on quantum vulnerabilities to the NCFs. That research was, in turn, aimed to understand the urgent vulnerabilities and NCFs that are most crucial to address first and the three NCF areas to prioritize for both public-private engagement and collaboration.

Building on those findings, CISA is now encouraging all critical infrastructure owners to follow the Post-Quantum Cryptography Roadmap, together with the guidance in the latest CISA Insight.

The Roadmap includes actionable steps organizations should take, including conducting an inventory of cur-

rent cryptographic technologies, creating acquisition policies regarding post-quantum cryptography, and educating their workforce about the upcoming transition.

The CISA Insight builds upon the Roadmap and provides additional information about a series of topics connected to post-quantum cryptography, from basic definitions of the technology to why and how it can be a threat to existing computer systems.

The document also includes a list of additional resources for critical infrastructure and government network decision-makers to learn more about post-quantum cryptography.

"Critical infrastructure and government leaders must be proactive and begin preparing for the transition to post-quantum cryptography now," Harrington concluded.

The CISA Insight comes weeks after the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) selected the first-ever group of encryption tools that could potentially withstand the attack of a quantum computer.

6.Samsung SDS to join NIST's post-quantum cryptography project

by Lee Ji-yoon
https://www.koreaherald.com/view.php?ud=20220825000568

Samsung SDS said Thursday it is joining a post-quantum cryptography project led by a cybersecurity center at the National Institute of Standards and Technology in the US, along with a slew of global tech firms like Amazon Web Service, Cisco and Microsoft.

The project, called Migration to PQC or post-quantum cryptography, aims to replace the current cryptographic algorithms, especially public-key cryptography, to better protect digital information in the era of quantum computing.

Once access to practical quantum computers becomes available, the company said, all public-key algorithms and associated protocols will be vulnerable to criminals and competitors. The project develops replacement of hardware, software and service that are resistant to quantum computer-based attacks.

Samsung SDS, the sole participant from South Korea, will adopt its own firewall product using cryptographic algorithm detection technology developed by its subsidiary Secui. The technology is designed to detect vulnerable cryptographic algorithms in numerous devices and applications in network infrastructures.

The company also plans to offer support for its cloud clients in their shift to quantum-resistant algorithms across their cloud infrastructures and applications.

Adding to post-quantum cryptography, Samsung SDS said it has secured its prowess in homomorphic encryption, another security technology for quantum computing that analyzes encrypted data without access to the secret key.

"Samsung SDS' joining the NIST project is a recognition of its technological prowess in the field of security," said Lee Sang-wook, senior vice president at Samsung SDS. "We will ramp up efforts to come up with quantum-resistant products and services in collaboration with other participating companies in the project."

7.China's Baidu enters quantum computing chat with Qian Shi system

by Tobias Mann
https://www.theregister.com/2022/08/25/china_baidu_quantum_computing/

Chinese search giant Baidu has unveiled its first quantum computing hardware and software capabilities during the Quantum Create developer conference in Beijing this week.

The system, dubbed Qian Shi, which means "the origin of all things is found in the heavens," is a superconducting quantum computer, which Baidu says is capable of 10 qubits of processing power. The search provider is billing the system a research platform that will allow users to explore practical applications for quantum computing without requiring direct access to the physical hardware.

“With Qian Shi and Liang Xi, users can create quantum algorithms and use quantum computing power without developing their own quantum hardware, control systems, or programming languages,” Runyao Duan, director of the institute for Quantum Computing at Baidu Research, said in a statement.

The development represents the culmination of four years of research and development by Baidu’s Institute for Quantum Computing. The division has already begun work on Qian Shi's successor, which Baidu says will feature 36-qubit superconducting quantum chip with couplers

According to Daniel Newman, principal analyst and founder of Futurum, Qian Shi is a significant step for Baidu, which has already shown meaningful progress in other disruptive technologies like AI and autonomous vehicles.

“Is it significant for Baidu, yes. Is it going to be immediately valuable in solving extraordinarily complex problems? The answer is probably not,” he said, explaining that much of the emphasis around quantum computing has been academic or experimental and has only recently moved toward practical applications of the tech.

Baidu appears to be aware of this challenge and has developed a software platform for quantum computers, called Liang Xi, that enables access to quantum services via mobile app, PC, or the cloud. At launch the search provider says the system supports both its Qian Shi system and the trapped ion quantum device developed by the Chinese Academy of Sciences.

Baidu believes this combination of hardware, software, and accessibility will speed the design and development of new materials and study of biological functions that have traditionally relied on high-performance computing. The company cites battery development and protein-folding simulations as opportunities for quantum computing development.

Baidu's idea resembles that of university computer labs from the 1970s, where limited compute resources are shared amongst researchers. It's an approach that several quantum computing and cloud providers have employed in recent years to advance the tech.

Recent examples include D-Wave’s decision to open its next-gen Advantage2 systems to the public by way of a cloud subscription service. The offering provides access to a 500 qubit system, however the full Advantage2 system is expected to deliver closer to 7,000 qubits of performance when it arrives in the next couple of years.

Similarly Microsoft Azure tapped IonQ, a relative newcomer to the quantum realm, earlier this month to expand its quantum computing capabilities.

Meanwhile, IBM continues to advance its own cloud-based Quantum computing systems and services in recent

months with the announcement of a 4,158-qubit system slated to launch in 2025.

While much of the quantum conversation continues to be academic, as quantum computing becomes more accessible and continues to evolve, Newman expects to see more applications of the tech become more tangible.

8.11 Top Experts: Quantum Top Trends 2023 And 2030

by Stephen Ibaraki
https://www.forbes.com/sites/stephenibaraki/2022/08/19/11-top-experts-quantum-top-trends-2023-and-2030/?sh=12f3266a69f9

Quantum Information Science/Quantum Computing (QIS / QC) continues to make substantial progress into 2023 with commercial applications coming where difficult practical problems can be solved significantly faster using QC (quantum advantage) and QC solving seemingly impossible problems and test cases (not practical problems) that for classical computers such as supercomputers would take thousands of years or beyond classical computing capabilities (quantum supremacy). Often the two terms are interchanged. Claims of quantum advantage or quantum supremacy, at times, are able to be challenged through new algorithms on classical computers.

The potential is for hybrid systems with quantum computers and classical computers such as supercomputers (and perhaps analog computing in the future) could operate in the thousands and potentially millions of times faster in lending more understanding into intractable challenges and problems. Imagine the possibilities and the implications for the benefit of Earth's ecosystems and humankind significantly impacting in dozens of areas of computational science such as big data analytics, weather forecasting, aerospace and novel transportation engineering, novel new energy paradigms such as renewable energy, healthcare and drug discovery, omics (genomics, transcriptomics, proteomics, metabolomic), economics, AI, large-scale simulations, financial services, new materials, optimization challenges, ... endless.

The stakes are so high in competitive and strategic advantage that top corporations and governments are investing in and working with QIS / QC. (See my Forbes article: Government Deep Tech 2022 Top Funding Focus Explainable AI, Photonics, Quantum—they (BDC Deep Tech Fund) invested in QC company Xanadu). For the US, in 2018, there is the USD $1.2 billion National Quantum Initiative Act and related U.S. Department of Energy providing USD $625 million over five years for five quantum information research hubs led by national laboratories: Argonne, Brookhaven, Fermi, Lawrence Berkeley and Oak Ridge. In August 2022, the US CHIPS and Science Act providing hundreds of millions in funding as well. Coverage includes: accelerating the discovery of quantum applications; growing a diverse and domestic quantum workforce; development of critical infrastructure and standardization of cutting-edge R&D. Quantum specific programs are: Quantum Science Network (lead agency: DOE); Quantum User Expansion for Science and Technology Program (DOE); Quantum Networking and Communications Research and Standardization (NIST); Next Generation Quantum Leaders Pilot Program (NSF) — annual authorized investment USD $153 million.

To gain perspective on where QIS / QC is going, I reached out to QIS / QC experts for their views.

Thus, top quantum experts give their top 3 QIS / QC trends for 2023 and 2030. I tried to keep their phrasing as close to their submissions to me as possible thus you will see their insights on 2023 and 2030 with the phrasing differing in their descriptions.

In addition, interviews with many of the experts are spotlighted where you can gain their deep insights in QIS / QC. The interviews can be found with the non-profit IEEE TEMS (interviews by Stephen Ibaraki; go to the general listing of all interviews and then use the browser Find option to search on a name). Interviewees, with

a combined 10 hours of dialogue, include: Steve Brierley, Mark Saffman, Travis Humble, Gopal Dixit, Sebastian Weidt, Michele Mosca, whurley, Scott Aaronson, Stefan Woerner, Hausi Müller. There are direct links to the interviewees profile page and video where they have provided their trends below.

Many of the QIS / QC experts are also speaking at IEEE Quantum Week QCE22 September 18-23, 2022.The IEEE, Institute of Electrical and Electronic Engineers, its roots dating back to 1884, and with more than 420,000 members in 160-plus countries, is the world's largest non-profit technical professional organization dedicated to advancing technology for the benefit of humanity.

Basic principles

Quantum Physics produces Quantum Effects from Quantum Mechanics providing Quantum Information Science and related technologies (QIST) that includes quantum computing, quantum simulation, quantum communications, quantum sensing, quantum measurement, quantum materials...this has spawned areas such as quantum safe cryptography and more. I often use QC as the general term for simplicity to point to Quantum Effects-related to Quantum Information Science and related technologies. Quantum Information Science or Quantum Information Science and Technology (QIST) is the better umbrella term.

The University of Waterloo Institute for Quantum Computing does a good overview on QIST with definitions. Microsoft, IBM, Google, and other large technology companies also provide good overviews including their work in QC.

A basic measure of QC capability is the number of quantum bits (qubits), the fundamental unit used to store and process data. Digital computers use bits which are like a light switch, on or off. Qubits can store a linear combination of one and zero (called superposition) encoding, an infinite number of possible states in each individual qubit creating powerful capabilities. While two bits represent two states in the classical computer, two qubits together can be in four different states. For n qubits the number of states increases by 2 to the nth power (2^n). So, for a 10-qubit configuration, this becomes 2^10 combinations; for 32 qubits, 2^32 combinations—that's more than four billion. That's much better than 32 digital bits that are either one or zero. The added quantum properties of entanglement where qubits work in perfect tandem, leads to exponential computing capabilities not possible even with the fastest zetascale (thousand billion billion) next generation supercomputers. Exascale supercomputers released in 2021 can do more than 1 billion-times-billion calculations per second or more than 1000 petaflops.

Qubits are rather unstable and noisy—break down or decohere before they can do something useful—one of the fundamental challenges with QC. There are ways to address this though we are still in the early days. So, when qubit figures are published for quantum machines they are usually in terms of stable qubits or logical qubits.

IBM, believes these published figures are not meaningful so have proposed another number, Quantum Volume. Quantum Volume (QV) combines qubits with connectivity between the bits and quality. IonQ believes the QV numbers are too large so have come up with a measure for their Algorithmic Qubits which is log 2 of QV.

There is also this concept of noisy intermediate-scale quantum (NISQ) where QC can contain hundreds of qubits (of moderate gate fidelity) but haven't achieved fault-tolerance (don't continuously implement quantum error correction so challenging to use for practical applications) and are not sufficiently large to solve practical applications (coined by John Preskill in 2018, see Wikipedia for more on these areas). You will also see the term, Quantum key distribution (QKD), which is a secure communication method involving quantum mechanics.

This article is based upon insights from my daily pro bono work, across more than 100 global projects and communities, with more than 400,000 CEOs, investors, scientists, and notable experts.

QIS / QC 2023 & 2030 Trends

- Alan Baratz, CEO, D-WAVE Systems Inc.

  - Top 3 QIS / QC trends for 2023

    1. Commercialization of quantum computing emerges (real customers, real revenue, real products).
    2. Quantum hybrid optimization applications begin to go into production.
    3. It will become widely accepted that NISQ systems will not deliver commercial value - Error correction will be required.

  - By 2030

    1. Scalable, error-corrected gate-model machines will begin to emerge (operative word is scalable).
    2. Clear set of "killer apps" are emerging.
    3. Quantum is commercial and mainstream – it's on every CIO/CTO's roadmap, much like the emergence of cloud computing or AI.

- Sebastian Weidt - CEO and Co-founder - Universal Quantum (interview)

  - 2023

    1. Focus will shift towards identifying and supporting quantum computing hardware approaches that can get out of NISQ and really can reach utility-scale using currently available engineering.
    2. With the knowledge of the threads to data security that come with quantum computing becoming ever more prevalent, QKD adoption include QKD-on-a-chip will soar.
    3. We will see a significant increase of government involvement in quantum computing via investment as well as via national protection mechanisms.

  - 2030

    1. We will have access to utility-scale quantum computing, delivering transformational capabilities to end-users.
    2. We will see broad adoption across a wide variety of industry sectors, leading to life-changing products and disruptive changes to the markets.
    3. We will have the first 'quantum war' – State actors and others will use quantum computers to try and protect their national and international interests, threatening the world order as we know it.

- Mark Saffman: Professor of Physics at the University of Wisconsin-Madison; Director of the Wisconsin Quantum Institute; Chief Scientist for Quantum Information at ColdQuanta, Inc (interview)

  - My top 3 trends for 2023

    1. Continued progress on demonstrations of quantum error correction going below code thresholds.
    2. Reaching quantum advantage in the combination of quantum sensors with small quantum processors.
    3. Emergence of neutral atom quantum computers as a scalable approach.

  - By 2030 I expect to see

    1. Computers with 100 logical qubits that provide beyond classical computational capabilities.
    2. Widespread deployment of secure quantum communication networks.
    3. Quantum enhanced inertial navigation systems that operate independent of GPS.

- Scott Aaronson: David J. Bruton Centennial Professor of Computer Science at the University of

Texas at Austin; recipient of ACM Prize in Computing (interview)

- As the three trends I'm most excited about for 2023 (among the ones that can be foreseen), I'll pick

1. Verifiable Quantum Advantage on Near-Term Devices.
2. Experimental Progress Toward Useful Quantum Error-Correction.
3. Discovery of More Efficient Error-Correcting Codes and Fault-Tolerance Schemes.

- 2030: Is too far in the future for me to say.

- Travis Humble: Deputy Director at the Department of Energy's Quantum Science Center; Distinguished Scientist at Oak Ridge National Laboratory; Director of the lab's Quantum Computing Institute (interview)

- I see the following ideas as key trends coming in 2023

1. Experimental demonstrations in quantum signal processing.
2. Rapid growth in quantum-error corrected processing.

- In the long term, 2030, I have my eyes set on

1. Fault-tolerant operation of quantum computing systems.
2. Cryogenically integrated quantum computing and HPC systems with local quantum networks.

- Michele Mosca: Co-founder, Institute for Quantum Computing, University of Waterloo; Founder of Quantum-Safe Canada and Quantum Industry Canada; Co-founder and CEO of the quantum-safe cybersecurity company, evolutionQ (interview)

- Top 3 trends for 2023

1. Quantum cyber vulnerability scanning and risk assessment become best-practices for cyber risk managers and IT procurement.
2. Increasing engagement from end-users (with computational challenges) with quantum software companies to explore potential enhancements from future quantum computers.
3. Increasing policy discussions and debates around national quantum strategies, balancing international cooperation and development of global markets with desire to develop domestic industries.

- Top 3 trends for 2030

1. Quantum-safe cryptography, including post-quantum public key infrastructure and certified QKD networks, deployed across main digital platforms.
2. Benchmarking the increasing power of fault-tolerant quantum computers; approaching quantum advantage via fault-tolerant QCs.
3. Quantum sensing technologies impacting several industry verticals.

- Steve Brierley: Founder and CEO of Riverlane (interview)

- 2023 trends

1. Error Correction: This is such an uber-trend it both trumps and encompasses all others. Error correction is the key that will unlock useful quantum computing in the future. Qubits (of all types) are delicate, unstable and prone to high volume of errors that can quickly overwhelm the system.

Decoding these even on a 'small' quantum computer requires real-time identification and correction of billions of errors (equivalent to Netflix' total streaming volume, for ex) per micro second. This is a known challenge but until now the industry has collectively put it in the bucket labelled 'too hard – figure it out in the future'. That future begins now. Google and Quantinuum have recently performed successful experiments to create 'logical qubits' (a stable virtual qubit made up from many physical qubits). End users, including governments, are now demanding (and funding) concrete steps toward error-corrected quantum computer systems with logical qubits. Riverlane is now soft launching its 'decoder' (the layer of the quantum stack that identifies and corrects the billions of system errors in real time) across various qubit and hardware types. Because error correction has always been our single minded mission and focus, our decoder will stand apart from any similar capability in the global market (we'll do demos and publish open peer reviewed data in Q4 and 2023 clearly substantiating this). Whether quantum hardware companies use our decoder or their own in their stack, 2023 will be the year when the global quantum community turns its collective attention fully to post NISQ, error-corrected quantum computing. It's a complex long term problem – perhaps the most challenging yet undertaken by the human race – so this will remain a focus into 2030 and beyond.

2. Quantum Networks: Quantum networks transmit and share digital information much like classical networks but use qubits so are potentially far more powerful. Due to their enormous complexity and the error problem identified above, quantum networks don't yet fully exist but that's starting to change and will accelerate in 2023 as scientists build and test prototype systems. Their first use case are likely to be unhackable communications secure for IT security, banking and medicine et al. Quantum networked use cases like quantum key distribution are already helping secure data transmissions over short distances.

3. Qubits: There are many different types of qubits, each with their own pros and cons. Today they tend to fall into two broad buckets 1) atomic (ion traps, neutral atoms) and 2) solid state (particularly superconducting qubits) with 'photonic' qubits potentially forming a distinct third category. One version of 'conventional wisdom' (if such a thing exists in a field so new and complex) has been that qubits are an arms race where one technology will emerge as winner. Expect that hypothesis to start to be debunked in 2023 as more exotic types of qubits (for ex, topological and silicon) emerge. So we'll likely pivot in 2023 from the arms race model to one where a variety of qubits have a place in a future quantum computing ecosystem with different types of qubits ideal for different types of use cases.

- 2030: Harder question but 2023 tends will continue for many years.

- Dr. Stefan Woerner, Principal Research Scientist, Manager, Quantum Applications Research & Software, IBM Quantum, IBM Research Europe – Zurich (interview)

  - Statements: These statements reflect what the IBM Quantum team has laid out in our roadmap, which was recently updated through 2025.
  - Near-term

    1. Advanced error mitigation techniques will further improve the performance of today's noisy quantum devices and show a continuous path towards the ultimate goal of fault tolerant quantum computers.
    2. Soon, we could see the first demonstrations of using quantum computers to perform tasks that are provably intractable for classical computers. Then, further advancements on error mitigation, algorithms, and circuit knitting techniques will lay the groundwork for industry to move toward the first applications with a quantum advantage that benefits business and science.
    3. Alongside the promise of quantum computing is the potential for future quantum computers to decrypt today's data and classical systems. However, after six years of evaluation, the US National Institute of Standards and Technology (NIST) announced the first four standards for quantum-

safe cryptography protocols. These algorithms, three of which IBM was directly involved in developing, effectively protect against this eventuality. The topic has already gained significant traction, as governments and companies are exploring, and starting to integrate these protocols into their processes and IT infrastructure. This will be crucial to become quantum safe and prepare for the future.

- Long-term

1. Throughout the next years, quantum hardware will significantly improve in scale, quality, and speed. Together with research in error mitigation and error correction this will lead to advances towards fault tolerant quantum computers of increasing scale.
2. We already know how some quantum algorithms and possible applications of quantum computers could soon be relevant to problems in many domains. However, this is likely only the tip of the iceberg. After first demonstrations of quantum advantage through noisy devices, and significant advances towards building fault tolerant quantum computers, we'll also see more algorithmic breakthroughs and new applications with large impact for business and society.
3. Quantum computers will be used in more and more domains to accelerate certain tasks via cloud access. Their use becomes more natural and tightly integrated in an increasing number of services. So, it is important for students, developers, and domain experts to begin developing knowledge and skills in quantum, and industries begin to develop their quantum workforce.

- Rafael Sotelo, PhD., Quantum-South, President; Universidad de Montevideo, Director of Research

- 2023

1. We will see more Proof of Concept of Quantum Computing use cases in different areas of human activity.
2. Pilots and implementations in production of Quantum Computing or quantum inspired algorithms in industries will be known, particularly in certain optimization applications to air and maritime cargo logistics.
3. New approaches to hardware will begin to be studied, with mixed systems, partly based on quantum states of matter, with longer lifetimes that will provide memory to the systems, and on the other hand, processing and communication will be based on states of the light.

- 2030

1. QC will be widely used in large optimization problems in logistics and industrial organization, as well as in consumer technology-oriented services, such as recommender systems, data analysis, Smart cities, IoT, and others.
2. Some manufacturers will comply with their today roadmaps and there will be large quantum computing systems.
3. New mixed technologies (matter-light) will continue to be experimentally developed as physical support for quantum computing and will prove viable and promising.

- Hausi A. Muller, Professor, Department of Computer Science, University of Victoria; General Chair IEEE Quantum Week 2023 (QCE23); IEEE Quantum Week 2022, QCE22 Finance Chair, QCE22 Workshops Co-Chair; Co-Chair IEEE Future Directions Quantum Initiative (interview)

- 2023

1. Quantum error correction (QEC) for quantum fault-tolerant computing. The major quantum computing companies are all working passionately on hardware and software QEC.

2. Quantum runtimes to integrate quantum and classical computations. Different aspects of a quantum problem are best solved by having classical and quantum computers collaborate and going back and forth in the course of algorithmic solutions.
3. Appetite for knowledge of quantum computing and quantum information is increasing dramatically. Educational institutions and companies are eager to train students and developers in quantum engineering.

- 2030

1. The quest toward 300 logical qubits — fault-tolerant, error-corrected qubits with high fidelity and coherence.
2. Software packages for solving quantum optimization problems.
3. Practical and effective quantum simulation of molecular structures.

- Chintan Oza, Founder of Anantam Ecosystems & Regional Director of India at Founder Institute

- 2023

1. Start of Quantum Transformation in Enterprise: more and more processes would be made quantum ready.
2. Semantic Web: Extension of Quantum Computing beyond earth: At present thousands of satellites are connected with AWS/Azure/Google Cloud. Hence, Cloud Computing is available and is being extended to semantic web.
3. Research for Humanity: Quantum would play major role in formulation of new materials as well as R&D of pharma to help fight from ongoing and future pandemic.
4. Rise of Quantum Encryption driven token economy: New token driven use cases would be supported by Quantum grade encryption in various IoT devices.
5. Quantum in Syllabus: Quantum would be taught as a subject in most engineering undergraduate schools.

- 2030

1. Global operation of Smart Communities/Fleets: Rise of life in an Algorithmic world.
2. Governance: Governments would adopt Quantum Computing in e-governancce.
3. Real Convergence: Beyond 2025, convergence of multiple emerging tech like Quantum and Metaverse would provide new use cases and business models.

9.Compact QKD system paves the way to cost-effective satellite-based quantum networks

by Optica
https://www.sciencedaily.com/releases/2022/08/220818102732.htm

Researchers report an experimental demonstration of a space-to-ground quantum key distribution (QKD) network using a compact QKD terminal aboard the Chinese Space Lab Tiangong-2 and four ground stations. The new QKD system is less than half the weight of the system the researchers developed for the Micius satellite, which was used to perform the world's first quantum-encrypted virtual teleconference.

The demonstration represents an important step toward practical QKD based on constellations of small satel-

lites, a setup considered one of the most promising routes to creating a global quantum communication network.

"QKD offers unconditional security by using single photons to encode information between two distant terminals," said research team member Cheng-Zhi Peng from the University of Science and Technology of China. "The compact system we developed can reduce the cost of implementing QKD by making it possible to use small satellites."

Peng and researchers from other institutions in China describe their new system and experimental results in Optica, Optica Publishing Group's journal for high-impact research. They also found that QKD performance can be boosted by building a network of satellites orbiting at different angles, or inclinations, in relation to the equator.

"Our new work demonstrates the feasibility of a space-ground QKD network based on a compact satellite payload combined with constellations of satellites with different orbit types," said Peng. "In the near future, this type of QKD system could be used in applications that require high security such as government affairs, diplomacy and finance."

Shrinking the QKD system

QKD uses the quantum properties of light to generate secure random keys for encrypting and decrypting data. In previous work, the research group demonstrated satellite-to-ground QKD and satellite-relayed intercontinental quantum networks using the Micius satellite. However, the QKD system used aboard that satellite was bulky and expensive. About the size of a large refrigerator, the system weighed around 130 kg and required 130 W of power.

As part of China's quantum constellation plan, the researchers sought to develop and demonstrate a more practical space-ground QKD network. To do this, they developed a compact payload that allowed the Tiangong-2 Space Lab to act as a satellite QKD terminal. The QKD payload -- consisting of a tracking system, QKD transmitter and a laser communication transmitter -- weighed around 60 kg, required 80 W of power and measured about the size of two microwave ovens.

"This payload was as integrated as possible to reduce volume, weight and cost while achieving the high performance necessary to support space-to-ground QKD experiments," said Peng. "It also had to be very durable to withstand harsh conditions such as the severe vibration experienced during launch and the extreme thermal vacuum environment of space."

The researchers performed a total of 19 QKD experiments during which secure keys were successfully distributed between the Space Lab terminal and four ground stations on 15 different days between October 2018 and February 2019. These experiments were conducted at night to avoid the influence of daylight background noise.

The researchers found that the medium (~42°) inclination orbit of the space lab allowed multiple passes over a single ground station in one night, which increased the number of keys that could be generated. They also built a model to compare the performance of satellite-based QKD networks with different orbit types. They found that combining satellites with a medium-inclination orbit like the space lab with a sun-synchronous orbit that travels over the polar regions achieved the best performance.

Next steps

The researchers are now working to improve their QKD system by increasing the speed and performance of the QKD system, reducing cost, and exploring the feasibility of daytime satellite-to-ground QKD transmission. "These improvements would allow a practical quantum constellation to be created by launching multiple low-

orbit satellites," said Peng. "The constellation could be combined with a medium-to-high-orbit quantum satellite and fiber-based QKD networks on the ground to create a space-ground-integrated quantum network."

Although not part of this work, an even smaller quantum satellite developed by Hefei National Laboratory and University of Science and Technology of China and other research institutes in China was successfully launched into space on July 27. This satellite, known as a micro/nano satellite, weighs about a sixth the weight of the Micius satellite and contains a QKD system that is about a third of the size of that demonstrated in the Optica paper. That satellite is designed to carry out real-time satellite-to-ground QKD experiments, representing another important step toward low-cost and practical quantum satellite constellations.

10.Google's quantum supremacy challenged by ordinary computers, for now

by Matthew Sparkes
https://www.newscientist.com/article/2333837-googles-quantum-supremacy-challenged-by-ordinary-computers-for-now/

Google has been challenged by an algorithm that could solve a problem faster than its Sycamore quantum computer, which it used in 2019 to claim the first example of "quantum supremacy" – the point at which a quantum computer can complete a task that would be impossible for ordinary computers. Google concedes that its 2019 record won't stand, but says that quantum computers will win out in the end.

Sycamore achieved quantum supremacy in a task that involves verifying that a sample of numbers output by a quantum circuit have a truly random distribution, which it was able to complete in 3 minutes and 20 seconds. The Google team said that even the world's most powerful supercomputer at the time, IBM's Summit, would take 10,000 years to achieve the same result.

Now, Pan Zhang at the Chinese Academy of Sciences in Beijing and his colleagues have created an improved algorithm for a non-quantum computer that can solve the random sampling problem much faster, challenging Google's claim that a quantum computer is the only practical way to do it. The researchers found that they could skip some of the calculations without affecting the final output, which dramatically reduces the computational requirements compared with the previous best algorithms.

The researchers ran their algorithm on a cluster of 512 GPUs (graphics processing units), completing the task in around 15 hours. While this is significantly longer than Sycamore, they say it shows that a classical computer approach remains practical.

They also calculated that if they were able to run their algorithm efficiently on an exascale supercomputer – which isn't a given, as there are performance overheads in translating code for these machines – it could solve the problem in "a few dozens of seconds", beating Sycamore's time. The first public exascale machine only went online this year, though some are thought to be operating in private.

Ashley Montanaro at the University of Bristol, UK, says that although the improvements to the classical algorithm are impressive, comparing quantum hardware from 2019 with cutting-edge classical hardware like an exascale supercomputer ignores the probable gains in quantum computing research over the past three years.

"I think it was always sort of clear at the time that Google did their experiment that there was going to be some development of better classical algorithms that would somehow try to compete with the quantum computer because Google sort of stuck their heads above the parapet," he says.

Zhang says that his team's algorithm is "massively more efficient than existing methods" but also concedes that classical computers are unlikely to keep pace with quantum machines for certain tasks. "Eventually quantum

computers will display overwhelming advantages over classical computing in solving specific problems," he says.

The study from Zhang's team isn't the first challenge against Google's claim, although it is perhaps the strongest. After Google's announcement in 2019, IBM claimed that Summit could have completed the task in two and a half days, but crucially it didn't run the experiment, even on a smaller scale as Zhang's team did.

In a statement, Sergio Boixo, principal scientist at Google Quantum AI, said: "In our 2019 paper we said that classical algorithms would improve… but the key point is that quantum technology improves exponentially faster. So we don't think this classical approach can keep up with quantum circuits in 2022 and beyond, despite significant improvements in the last few years."

11.Montreal-based Company Finalizes Design of its First Blockchain Application in QRNG Technology, Predicting Prototype Release For Next Year

by JAMES DARGAN
https://thequantuminsider.com/2022/08/16/montreal-based-company-finalizes-design-of-its-first-block-chain-application-in-qrng-technology-predicting-prototype-release-for-next-year/?utm_source=newsletter&utm_medium=email&utm_term=2022-08-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Working+in+Quantum+Quantum+Earnings+Season+And+More+Quantum+News

Prototype

Quantum eMotion Inc., a Montreal, Canada-based quantum company, has announced the completion of the design of its first Blockchain application in Quantum Random Number Generator (QRNG) technology. Eyeing a 2023 release of the prototype according to a statement from CEO Francis Bellido, the company's patented solution for a QRNG exploits the built-in unpredictability of quantum mechanics and promises to provide enhanced security for protecting high-value assets and critical systems. The company's core customer base is focused on financial services, Blockchain applications, cloud-based IT security infrastructure, classified government networks and communication systems, secure device keying, and quantum cryptography markets.

Founded as Quantum Numbers Corp Quantum eMotion Corp. back in 2007, the company changed its name to Quantum eMotion Inc. in June 2021. With a mission to address the growing demand for affordable hardware security in connected devices, the company's patented solution—which it has reported they are making "significant progress" on—for a QRNG exploits the built-in unpredictability of quantum mechanics and promises to provide enhanced security for protecting high-value assets and critical systems.

Mitacs Funding

Early last year, Quantum eMotion received funding from Mitacs, a Canadian nonprofit national research organization, for Blockchain applications of its QRNG2 technology, and used the funds to further develop the use of the QRNG2 device to harden the cryptographic mechanisms of hardware cryptocurrency wallets, and for using QRNG as a "verifiable randomness beacon" for Blockchain oracle.

"We are very excited to announce the decisive progress made in our three Blockchain programs and more particularly, the design completion of the hardware cryptocurrency wallets integrated with our QRNG2," said

Quantum eMotion's CEO Francis Bellido in a statement.

"This will be the first Hardware Crypto Wallet able to store private keys for cryptocurrencies offline in a quantum-encrypted device, which will make these new wallets inviolable for the hackers."

12.Getting ready for post-quantum security mayhem

by Nitin Dahad
https://www.embedded.com/getting-ready-for-post-quantum-security-mayhem/

There's a lot of work going on to address the potential for security mayhem in the post-quantum world, when many of the public-key encryption systems in place today could be easily broken. As the U.S. National Institute of Standards and Technology (NIST) highlights, "If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere."

In a recent interview with embedded.com, Joppe Bos, senior principal cryptographer at NXP Semiconductors, explained why we should be worried. He said, "Quantum computing has the potential to destroy security as we know it." He added, "As the world becomes more connected and more data-driven, ensuring data and devices remain secure, even against quantum computers, is crucial. As NIST moves forward with developing a new post-quantum standard, NXP will offer our deep knowledge in security, and specifically our algorithmic expertise, to fortify our products for a post-quantum future. We aim to contribute to the common standard so that our customers can achieve long-term security in their own products."

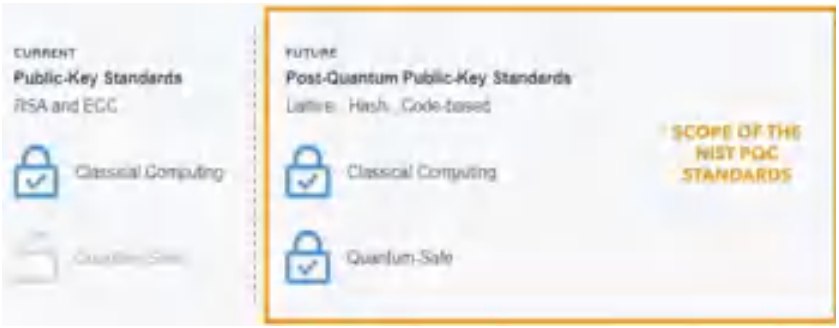
Many cybersecurity experts believe that when large-scale quantum computers come to fruition, the sheer computing power of these machines will be able to solve encryption challenges in a fraction of the time, breaking today's public key encryption systems and leaving data, digital signatures and devices vulnerable. This creates substantial security risks for online devices and data, including financial transactions, critical infrastructure, over-the-air update mechanisms, and more.

This is the why NIST has been working with industry to develop standardized post-quantum cryptography (PQC) algorithms, which would then help in the development of cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. As part of that process, in July 2022, NIST completed the third round of this PQC standardization process, selecting a total of four candidate algorithms for standardization, and four additional algorithms that will continue into the fourth round. The selected PQC algorithms will be used to develop a new public key encryption standard that is secure against both traditional and quantum computers.

The standards body recommends two primary algorithms to be implemented for most use cases: Crystals-Kyber (key-establishment) and Crystals-Dilithium (digital signatures); these were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications. Crystals-Kyber was submitted by NXP along with security experts from IBM. "The industry security experts of IBM, NXP and Arm, together with their academic partners (ENS, RAB, CWI and RUB) have created an industry-leading submission that will help shape the way we think about encryption and security for decades to come," said Michael Osborne, principal research scientist manager for foundational cryptography at IBM. "Kyber is not only faster than current standards, it provides our clients with strong security to protect systems and data as we enter the quantum era."

NXP's Bos said that the draft standards are expected in 2024, and so the company is working with customers already to consider what they need to be doing to migrate their products to implement the PQC algorithms

once they become standardized. The important factor to understand here is that PQC can run on classical computing hardware found in devices we use today and does not require a quantum computer. Bos said customers are already seeking advice on developing post-quantum ready security on their devices, and NXP has engaged with many customers already on this. "In industrial IoT, customers are already aware, and in automotive, cus-



tomers are getting nervous, so are also seeking advice."

Scope of the NIST PQC standards. Note that PQC can run on classical computing hardware found in devices today and does not require a quantum computer.

The Crystals-Kyber algorithm co-designed by NXP is expected to be part of the new key-exchange standard that will eventually replace current standards such as NIST SP 800-56A Rev. 3.

In addition to these, the signature schemes Falcon and Sphincs+ will also be standardized. Falcon will also be standardized by NIST since there may be use cases for which Crystals-Dilithium signatures are too large. Sphincs+ will also be standardized to avoid relying only on the security of lattices for signatures. NIST is asking for public feedback on a version of Sphincs+ with a lower number of maximum signatures.

Not related to SIKE break at KU Leuven

In recent weeks, there has been a lot of coverage of the work of researchers at KU Leuven, describing an attack whereby they were able to demonstrate the breaking of code of one of the proposed NIST PQC algorithms for the fourth round in an hour of single core computation (and the strongest parameter set) in less than 24 hours.

We asked Bos to provide some perspective on this. He commented, "Yes researchers from KU Leuven found a new attack on SIKE: this is one of the algorithms selected to proceed to a next round and might be considered for standardization. This is not one of the four selected algorithms for standardization."

"SIKE is an interesting approach based on isogonies, an approach very different from the lattice-based algorithms such as Kyber. This new attack was a surprise to the entire cryptographic community, and we congratulated the researchers at KU Leuven for this new approach. Their efforts and other, similar efforts by other researchers ensure that these algorithms are thoroughly tested to ensure they are able to protect against new and existing attacks."

"Although this new approach has no impact on any of the four selected PQC standards, from a technical point of view this does harm the perceived trust of the end-users in PQC in general. Trust is a fundamental property in security which is very hard to obtain and easy to lose. That is why we are working hard to build demonstrators and proof-of-concept together with our customers to show we as the industrial leaders in security have trust in the new post-quantum public-key standards."

13.WISeKey Implementing Post–Quantum Algorithms in its Secure Semiconductors

by JAMES DARGAN
https://thequantuminsider.com/2022/08/11/wisekey-implementing-post-quantum-algorithms-in-its-secure-semiconductors/?utm_source=newsletter&utm_medium=email&utm_term=2022-08-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+D-Wave+Hello+In+the+CHIPS+And+More+Quantum+News

WISeKey International Holding Ltd ("WISeKey "), a leading global cybersecurity, AI, Blockchain and IoT company, announces substantial progress in the implementation of post-quantum algorithms in its Secure Semiconductors MS6001/MS6003.

During the last two years, WISeKey has made substantial progress in developing post-quantum resistant algorithms by establishing strategic R&D partnerships with MINES Saint-Etienne Research Institute ("MINES Saint-Etienne"), an internationally renowned multidisciplinary university and lab created in 1816, aiming to help the international community find cryptography algorithms that will resist future quantum computing based cyber-attacks.

The WISeKey's team of experts is working with several NIST's candidates for the MS600X Common Criteria products: Crystals-Kyber for key exchange mechanism, and Crystals-Dilithium for signatures. The partnership is focusing into the practical implementation aspects for both algorithms, considering physical side-channel attack and deep learning process. This work completes the implementation of NTRU and ROLLO algorithms that the team has already studied, paving the way of a complete post-quantum cryptography toolbox.

This post-quantum cryptography toolbox will help to protect against the security threat posed by quantum computers, allowing hybrid solutions no later than 2025 as recommended by the French ANSSI. In addition to this, WISeKey will upgrade its PKI offer, adding new post-quantum features for the IoT market: Secure authentication, Brand protection, Network communications, future FIDO ("Fast IDentity Online") evolutions and additional generally web-connected smart devices that obtain, analyze, and process the data collected from their surroundings.

WISeKey is also working with NIST to define recommended practices for performing trusted network-layer onboarding, which will aid in the implementation and use of trusted onboarding solutions for IoT devices at scale. The WISeKey contribution to the project will be Trust Services for credentials and secure semiconductors to keep credential secure. Specifically, WISeKey will offer INeS Certificate Management Service (CMS) for issuing credentials and VaultIC secure semiconductors to provide tamperproof key storage and cryptographic acceleration.

While quantum computing offers endless perspectives to incredibly increase computing power, hackers will take advantage of this technology to crack cryptography algorithms, corrupt cybersecurity and compromise global economy. Research about quantum computing, namely how to use quantum mechanical phenomena to perform fast computation, was initiated in the early 1980s. The perspectives and unbelievable performances offered by this promising technology are so huge that many countries are sponsoring public/private R&D initiatives.

WISeKey brings its decades of expertise in designing Common Criteria EAL5+ and FIPS 140–2 Level 3 certified hardware-based secure elements (MS600x secure microcontrollers, VaultIC™, etc.) and in developing hacker-resistant firmware. The new algorithms to be evaluated will first have to practically run on WISeKey's existing and new hardware architectures. The Company will also share its expertise in deep learning AI techniques to prove the robustness of the implementations.

14.NTT Research & NTT Corporation Engage in Breakthrough Research at Crypto 2022

by JAMES DARGAN
https://thequantuminsider.com/2022/08/11/ntt-research-ntt-corporation-engage-in-breakthrough-research-at-crypto-2022/?utm_source=newsletter&utm_medium=email&utm_term=2022-08-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+D-Wave+Hello+In+the+CHIPS+And+More+Quantum+News

NTT Research, Inc., a division of NTT, today announced that members of its Cryptography & Information Security (CIS) Lab authored or co-authored 17 papers that are being delivered at Crypto 2022, one of the leading international conferences on cryptologic research. A paper co-authored by CIS Lab Director Brent Waters won the event's Best Paper Award, his second such award in the past three years. In addition, NTT Corporation and NTT Social Informatics Laboratories contributed another six papers. Organized by the International Association for Cryptologic Research (IACR), this year's hybrid event will take place in Santa Barbara, August 13–18. NTT Research is one of the conference's eight gold-level sponsors.

The Crypto 2022 program committee, comprised of more than 70 experts, accepted nearly 100 submissions this year. According to the posted conference program, the 23 papers associated with CIS Lab and other NTT cryptographers will be presented in sessions with the following topics: coding theory, distributed algorithms, idealized models, lattice-based signatures, lattice-based zero knowledge, lower bounds, post-quantum cryptography, quantum cryptography, secret sharing, secure hash functions, secure messaging and secure multi-party computation. Dr. Waters will present his paper, titled "Batch Arguments for NP and More from Standard Bilinear Group Assumptions" on Tuesday, August 16, at 11:20 (PST) during a session that acknowledges it with the conference's only Best Paper award this year. Two "best early career researcher papers" will also be recognized. Dr. Waters, who is also a professor of computer science at the University of Texas (UT) at Austin, was named CIS Lab Director in June, succeeding Dr. Tatsuaki Okamoto. At Crypto 2020, a paper co-authored by Dr. Waters won one of three Best Paper Awards given that year. (One of the other winners was co-authored by a senior researcher at NTT Secure Platforms Labs.) Dr. Waters' collaborator in this year's paper is Dr. David Wu, an assistant professor at UT Austin. Their breakthrough is to show how to batch the proofs of nondeterministic polynomial (NP)-class and other problems using standard assumptions and relatively non-complex techniques.

"It is exciting to see our CIS Lab and other parts of NTT engaged in so much cutting-edge research," NTT Research President and CEO Kazuhiro Gomi said. "Congratulations to Brent Waters and David Wu for their Best Paper Award, and the research itself, which appears to have such timely applications. Best wishes to all for a very productive conference."

The Waters-Wu paper introduces a new kind of proof system, which in cryptography consists of a proving party and a verifying party, where the prover is trying to convince the verifier of a "statement." Typically, the verifier relies on the prover to provide a witness. An example might be a digital signature, acting as a witness to the statement that a software update is not malware, but in fact produced by the vendor. In this paper, the authors develop techniques that allow for efficiently batching the transmission and verification of several statements. In so doing, they improve upon what Dr. Waters said are two main lines of prior work in this direction, namely: one that uses less standard and thus more risky computational assumptions for security; and the other, which uses certain types of lattice assumptions and probabilistic checkable proofs.

"In this work we show that batchable proof systems can be achieved from standard and well-studied assumptions on bilinear groups," Dr. Waters said. "Moreover, our techniques are very direct and show that complex probabilistic checkable proofs are not needed."

Two potential use cases involve the aggregation of signatures and the delegation of computation to cloud services. The first case relates to applications such as blockchains, in which each update consists of several signatures representing various transactions that users want to have processed. Instead of simply including all signatures from the transaction as part of an update (the default solution, which can incur a significant overhead), batchable verification enables aggregating these into one shorter object, the size of which is independent of the number of signatures included. The second case involves the increasingly large amounts of information storage

and processing being done via cloud services.

"The problem of delegation asks, how can I verify that a computation was performed correctly in a more efficient manner than simply performing it myself," Waters said. "Our work on batch argument systems can be immediately applied to tackle that problem."

The proceedings of the IACR's flagship conferences, which draw the world's leading cryptographers, are published by Springer in its Lecture Notes in Computer Science series. Dr. Yehuda Lindell, CEO and co-founder of Unbound Security, is scheduled to deliver this year's invited talk. To attend, see this registration page.

15.Quantum Cryptographic Scheme Might Create Counterfeit-Proof Cash

by Matt Swayne
https://thequantuminsider.com/2022/08/09/quantum-cryptographic-scheme-might-create-counterfeit-proof-cash/?utm_source=newsletter&utm_medium=email&utm_term=2022-08-26&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+D-Wave+Hello+In+the+CHIPS+And+More+Quantum+News

According to Notorious B.I.G., among other economists, mo' money necessarily correlates with mo' problems. However, a team of MIT and Harvard University researchers reports that quantum cash may solve at least some of those money problems, specifically counterfeiting, which costs the economy between $30 billion-$50 billion per year.

In a study published on ArXiv, the researchers suggest that the no-cloning theorem that rests at the heart of quantum mechanics can serve as part of a publicly verifiable quantum money protocol. The team of researchers includes Andrey Boris Khesin, Jonathan Z. Lu and Peter W. Shor, one of the pioneers of quantum computing algorithm design.

According to the researchers, a successful quantum money protocol would require three features: the efficient creation of money states, the efficient public authentication and unforgeability. This scheme would meet all three, they say. It includes the preparation of quantum states that can be efficiently authenticated by other parties — but would be impossible to counterfeit.

In the multiparty quantum cryptographic protocol, the mint can create quantum states which other participants in the system can verify but cannot duplicate. Specifically, the mint may generate the quantum money state associated with a serial number, which it releases publicly along with any other relevant information. Any party with the public information can then use a quantum computer to certify, the authenticity of the serial number without marginally changing the state.

This protocol is based on short-vector problem — SVP — on lattices. In other words, in order to counterfeit the state, the would-be hacker would have to solve the SVP, which is a well-studied problem in cryptographic circles.

According to the team: "In particular, our protocol uses a random lattice that contains one known short vector, and we show that anyone who can duplicate a quantum money state can find another, linearly independent, short vector in the lattice. This problem of finding a second short vector in a random lattice is equivalent to the short vector problem in a random lattice."

The quantum money state, itself, is a superposition of Gaussian balls.

"Assuming the SVP is hard, it is impossible to create a specific superposition of Gaussian balls, but it is possible

to create a random translate of a specific superposition," the researchers write.

The team offers several advantages of the approach.

They write: "Aside from its remarkable physical implications— an explicit example of a provably uncloneable quantum state—our quantum money also offers advantages unachievable by classical cryptocurrencies or physical bills. Since our money states are physical, they can serve as tangible yet unforgeable bills, but they could also be transferred through quantum channels as digital money. Moreover, verification of ownership can be done locally and offline, having no need for global synchronization through such mechanisms as blockchains."

Quantum money is just one of the outcomes of the protocol — there could be other uses. For example, the researchers said that it could lead to an antipiracy protocol that protects quantum computations — a circuit — from duplication.

They add: "One may also explore connections between quantum money and other branches of quantum cryptography, such as zero-knowledge proofs."

16.Indian Army focusses on Quantum computing to improve communication, gain edge over rivals

https://news.webindia123.com/news/Articles/India/20220805/3970372.html

To augment information secrecy, the Indian Army is focussing on leveraging Quantum Computing and is actively collaborating with the Industries and academia, who are the leaders in the field.

Top sources in the defence establishment informed that traditional computing and communications will be revolutionized when Quantum Computer is fully realized, which is an area of global Research and development (R&D) focus.

"Complex data computations which involve the processing of voluminous structured, as well as unstructured data using advanced algorithms, will be enormously eased with Quantum Computing and its associated technologies," said sources.

Indian Army is looking at this field of technology as a futuristic enabler for integrating a large density of C4I2SR components in the evolving battlefield, including sensors, communications platforms and information systems.

Comprehensive data fusion and decision support capability will be securely delivered to Commanders at various levels, with minimum latency and maximum effect. Whilst Quantum Computing offers wide applications in the commercial domains, the Indian Army is looking at active collaboration with Industry as well as academia, to evolve effective applications for computing, communications and cryptography

Indian Army has already taken the lead by way of establishing a Quantum Lab for evolving advanced concepts for applications and ushering further R&D on related technologies in collaboration with industry and academia. Information Warriors of the Army will be armed with the requisite knowledge which will facilitate in smooth induction of Quantum systems.

One of the key applications of Quantum Computing is in the area of Information secrecy. Traditional cryptographic systems will be completely or partially cracked with Quantum Computers in a matter of minutes. Such

a military capability will be a massive weapon at to threaten sensitive systems of any country, thereby threatening national sovereignty in multiple ways.

Therefore, there is an urgent requirement of replacing traditional cryptography with quantum-safe and quantum-resistant cryptographic methods. While Quantum Secrecy is a national interest, military information systems, which are currently based on hardware-based crypto platforms relying on mathematical computational complexity, will render Operational Information vulnerable to Quantum attacks by adversaries.

Quantum Key Distribution (QKD) involves the generation of highly advanced secrecy keys which can be effectively employed towards securing backbone networks. Since massive OFC infrastructure has already been created through Project NFS which has a pan India spread covering the entire Defence Network, the Indian Army is already prepared to embrace QKD on the infrastructure front. Fielding of QKD systems is expected to replace traditional backhaul secrecy with QKD, enhancing capacities of communication systems with enhanced cost efficiency as well as complete automation of key delivery.

Complete safety against Quantum attacks requires addressing the last mile. The development and deployment of indigenous Post Quantum Cryptography (PQC) algorithms is another area to focus on for Military Communications. While the country is aiming to achieve complete self-reliance in the field of Defence Communications, integration of PQC as an on-platform secrecy solution is required to concurrently evolve.

While the QKD and PQC will facilitate quantum secrecy and will provide a considerable edge to Operational as well as Tactical Communications, there is a requirement to impart core impetus for the indigenous development of Quantum Computer.

Futuristically, as the communication systems and applications evolve and integrate more and more systems, the core processing will need to be replaced in the Defence Data centres with Quantum Computers. While national R&D is focused in this field, the Indian Army is closely watching the advancements made by their adversaries, to ensure that these vital capabilities are inducted into our Armed Forces well ahead of time.

17.The time is now for quantum-safe security

by Bill Becker
https://gcn.com/emerging-tech/2022/08/time-now-quantum-safe-security/375431/

Agencies must understand what data is at risk and mitigate that risk with crypto-agile solutions as post quantum crypto standards are finalized.

Despite large scale quantum computing being several years away from being a practical reality, government experts are deservedly concerned about the cybersecurity implications today. The sooner an organization can lay the foundation for quantum cybersecurity, the better equipped it will be when bad actors start adding quantum hacking to their arsenal.

This was underscored in May 2022, when the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM 10) provided requirements and timelines for quantum-resistant cryptography. In announcing the memo, President Joe Biden noted that “America must start the lengthy process of updating our IT infrastructure today to protect against this quantum computing threat tomorrow.”

The memo continued by underscoring that “central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards.”

The concern for more immediate action in cryptographic agility is understandable. Even if a quantum computer

is a decade away, bad actors can take note of potential vulnerabilities now, and exploit them later.

Today's non-PQ (post-quantum) encryption absolutely will break (or be broken) in the future, affecting security features such as authentication, code-signing and digital signatures. If hackers can break the algorithm for the private key, they can, for example, impersonate the software update channel. What happens if an adversary gains the capability to "update" the firmware within an agency's IT infrastructure?

The quantum challenge: Data's necessary expiration date

Today's encrypted data has an expiration date. All data that is encrypted today using classic PKI-based cryptography is quantum vulnerable, with little if any protection against potential vulnerabilities that may become apparent later. Meanwhile, however, all of that data also has a timespan for which it must remain secure.

The data we encrypt today is already decaying, because its risk of exposure increases over time. When data encrypted data using current algorithms is transmitted over the network it becomes vulnerable to interception. Anyone with access to that data through surveillance, eavesdropping or hacking can harvest the data and store it until such a time that a quantum computer can decrypt it.

So what is there to do?

Recommended quantum safe transition strategy

When preparing for a quantum-safe encryption strategy, there are four things to keep in mind:

1. Quantum is coming. National Security Memo 10 emphasized the United States' commitment to continued technological and scientific leadership in quantum computing. Alongside the potential benefits of quantum computing are the acknowledged risks to the economy and national security since quantum computing will make PKI-based classic cryptography obsolete. The National Institute of Standards and Technology recently concluded a six-year effort and announced its selection of four quantum-safe algorithms designed to resist attacks from future quantum computers.

2. Know your risks. As already explained, long-term data is at risk to harvesting and early attacks. IT managers and other network professionals must assess their organizations' use of vulnerable cryptography, the expiration date of their encrypted data and the crypto maturity of their IT infrastructure.

   Several sources are available to explain risks and to plan ahead. NIST offers a publication titled "Getting Ready for Post-Quantum Cryptography" to help monitor standards development and perform risk assessment of where public-key crypto may be used in the infrastructure. It's essential to understand whether a network's equipment is crypto-agile.

   The National Cybersecurity Center of Excellence has recently launched its "Migration to Post Quantum Cryptography" Project. Understanding that replacement of cryptographic algorithms is both technically and logistically challenging, the NCCoE is undertaking a practical demonstration of technology and tools that can provide a head start on executing a migration roadmap in collaboration with a public and private sector community.

   Another excellent source of information is the National Security Agency's Post-Quantum Cryptography FAQ, which provides an excellent summary on the subject.

3. Focus on crypto-agility. Flexible upgradeable technology and a hybrid approach of classic and quantum-resistant crypto solutions is essential.

   Remember that crypto-agility is not about quantum; it's about being able to face the reality that all algo-

rithms fail with time. Many systems today make it difficult to rotate keys, to choose different sizes/parameters and to change mechanisms or key algorithms. These are all required for protocols to be versioned, negotiated and fail-safe when presented with unknown options. They are essential for crypto-agility, and it's important to work with providers with solutions that embrace those needs.

4. Start today. Preparation cannot be understated, which is why National Security Memo 10 made a point of it. Organizations must begin to design a quantum-resistant architecture today to protect against the emerging quantum threat. With IT infrastructure equipment often being deployed for years or decades without hardware replacement, it is important to make sure currently deployed hardware was developed with crypto-agility principles in mind and to deploy software or firmware updates once post-quantum crypto algorithms and protocols are standardized. It is also important to check with equipment providers to see what beta or technology preview firmware they have available for testing in non-production systems that implements pre-standardized quantum-resistant cryptographic algorithms. Testing will help identify performance or interoperability issues early and provide time to address the issues and mitigate the identified risks.

   Developing a quantum safe strategy must focus on understanding what data is at risk and mitigating this risk by deploying crypto agile solutions as we await finalization of post quantum crypto standards. Agencies should get started today so their strategy is in place well before large scale quantum computers are readily available.

18.Rigetti Awarded DARPA Contract for Quantum Application Benchmarking

by Bradford Williams, Polly Pearson
https://www.globenewswire.com/news-release/2022/08/04/2492411/0/en/Rigetti-Awarded-DARPA-Contract-for-Quantum-Application-Benchmarking.html

A subsidiary of Rigetti Computing, Inc. ("Rigetti" or the "Company"), a pioneer in full-stack quantum computing, has been selected by the Defense Advanced Research Projects Agency (DARPA) to develop benchmarks for quantum application performance on large-scale quantum computers. The program is worth up to $2.9 million over three years based on the achievement of certain milestones. Joining Rigetti on this project are the University of Technology Sydney, Aalto University, and the University of Southern California.

A key challenge of planning fault-tolerant quantum computers is the ability to predict their performance on target applications. Establishing rigorous and universal benchmarks could allow for more precise estimates on how fault-tolerant quantum computers could perform in the future. This program aims to produce a more detailed understanding of how errors occur at the qubit level, how those errors impact performance on target applications, and to provide an accurate estimation of how quantum hardware and software need to evolve to meet critical performance thresholds.

"We are proud to have been selected to deliver this critical program to advance quantum computing capabilities and benchmarks," said Chad Rigetti, founder and CEO of Rigetti Computing. "Rigetti continues to pioneer advances not only in quantum processor technology but also in applications and benchmarks. This award is a testament to our full-stack R&D capabilities and rigorous focus on delivering application performance. We believe having a set of industry-accepted application benchmarks will help mature the quantum computing ecosystem and inform our technology roadmap."

"I'm looking forward to assessing the impact of detailed models of superconducting qubits on the overall resources needed to create logical qubits," said Daniel Lidar, Viterbi Professor of Engineering at the University of Southern California. "Most of the existing work deals with somewhat simplified assumptions about qubit errors, and here we hope to improve the state of the art by building more faithful models of the qubits and their

environment."

"This is an extraordinary level of collaboration in the quantum software field," said Yuval Sanders, researcher at the Center for Quantum Software and Information at the University of Technology Sydney. "We will be developing some of the first automated software tools for quantum performance analytics that have ever existed. This will undoubtedly accelerate the field even further."

This award is part of DARPA's Quantum Benchmarking Program. The goal of the program is to re-invent key quantum computing metrics, make those metrics testable, and estimate the required quantum and classical resources needed to reach critical performance thresholds. The three-year project comprises two phases. Rigetti was awarded Phase 1, and the program includes an option for DARPA to award a second phase, concluding in February 2024.

19.Experiment with post-quantum cryptography today

by Bas Westerbaan, Christopher Patton, Peter Wu
https://blog.cloudflare.com/experiment-with-pq/

Practically all data sent over the Internet today is at risk in the future if a sufficiently large and stable quantum computer is created. Anyone who captures data now could decrypt it.

Luckily, there is a solution: we can switch to so-called post-quantum (PQ) cryptography, which is designed to be secure against attacks of quantum computers. After a six-year worldwide selection process, in July 2022, NIST announced they will standardize Kyber, a post-quantum key agreement scheme. The standard will be ready in 2024, but we want to help drive the adoption of post-quantum cryptography.

Today we have added support for the X25519Kyber512Draft00 and X25519Kyber768Draft00 hybrid post-quantum key agreements to a number of test domains, including pq.cloudflareresearch.com.

Do you want to experiment with post-quantum on your test website for free? Mail ask-research@cloudflare.com to enroll your test website, but read the fine-print below.

What does it mean to enable post-quantum on your website?

If you enroll your website to the post-quantum beta, we will add support for these two extra key agreements alongside the existing classical encryption schemes such as X25519. If your browser doesn't support these post-quantum key agreements (and none at the time of writing do), then your browser will continue working with a classically secure, but not quantum-resistant, connection.

Then how to test it?

We have open-sourced a fork of BoringSSL and Go that has support for these post-quantum key agreements. With those and an enrolled test domain, you can check how your application performs with post-quantum key exchanges. We are working on support for more libraries and languages.

What to look for?

Kyber and classical key agreements such as X25519 have different performance characteristics: Kyber requires less computation, but has bigger keys and requires a bit more RAM to compute. It could very well make the connection faster if used on its own.

We are not using Kyber on its own though, but are using hybrids. That means we are doing both an X25519 and Kyber key agreement such that the connection is still classically secure if either is broken. That also means that connections will be a bit slower. In our experiments, the difference is very small, but it's best to check for yourself.

The fine-print

Cloudflare's post-quantum cryptography support is a beta service for experimental use only. Enabling post-quantum on your website will subject the website to Cloudflare's Beta Services terms and will impact other Cloudflare services on the website as described below.

No stability or support guarantees

Over the coming months, both Kyber and the way it's integrated into TLS will change for several reasons, including:

1. Kyber will see small, but backward-incompatible changes in the coming months.
2. We want to be compatible with other early adopters and will change our integration accordingly.
3. As, together with the cryptography community, we find issues, we will add workarounds in our integration.

We will update our forks accordingly, but cannot guarantee any long-term stability or continued support. PQ support may become unavailable at any moment. We will post updates on pq.cloudflareresearch.com.

Features in enrolled domains

For the moment, we are running enrolled zones on a slightly different infrastructure for which not all features, notably QUIC, are available.

With that out of the way, it's…

20.Thousands of hackers flock to 'Dark Utilities' C2-as-a-Service

by Bill Toulas
https://www.bleepingcomputer.com/news/security/thousands-of-hackers-flock-to-dark-utilities-c2-as-a-service/

Security researchers found a new service called Dark Utilities that provides an easy and inexpensive way for cybercriminals to set up a command and control (C2) center for their malicious operations.

The Dark Utilities service provides threat actors a platform that supports Windows, Linux, and Python-based payloads, and eliminates the effort associated with implementing a C2 communication channel.

A C2 server is how adversaries control their malware in the wild, sending out commands, configurations and new payloads, and receiving data collected from compromised systems.

The Dark Utilities operation is a 'C2-as-a-service' (C2aaS) that advertises reliable, anonymous C2 infrastructure

and all the required additional functions for a starting price of just EUR 9,99.

A report from Cisco Talos says that the service has around 3,000 active subscribers, which would bring the operators a revenue of about EUR 30,000.

Dark Utilities emerged in early 2022 and offers full-blown C2 capabilities both on the Tor network and on the clear web. It hosts payloads in the Interplanetary File System (IPFS) - a decentralized network system for storing and sharing data.

Multiple architectures are supported and it appears that the operators are planning on expanding the list to provide a larger set of options of devices that could be targeted.

Cisco Talos researchers say that selecting an operating system generates a command string that "threat actors are typically embedding into PowerShell or Bash scripts to facilitate the retrieval and execution of the payload on victim machines."

The selected payload also establishes persistence on the target system by creating a Registry key on Windows, or a Crontab entry or a Systemd service on Linux.

According to the researchers, the administrative panel comes with multiple modules for various types of attack, including distributed denial-of-service (DDoS) and cryptojacking.

With tens of thousands of threat actors already subscribed and the low price, Dark Utilities is likely to attract an even larger crowd of less-skilled adversaries.

21.New Gmail Attack Bypasses Passwords And 2FA To Read All Email

by Davey Winder
https://www.forbes.com/sites/daveywinder/2022/08/04/gmail-warning-as-new-attack-bypasses-passwords--2fa-to-read-all-email/?sh=3b5635884128&utm_content=bufferad54a&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

Among the best practice items for Gmail security protection, strengthening your login credentials and enabling two-step verification are high on the list, as I mentioned in an article over the weekend. But what if I were to tell you that security researchers have now uncovered evidence of one likely state-sponsored attack group that has found a way to bypass even these protections?

North Korean hacking group can access Gmail without compromising login credentials

According to cyber security firm Volexity, the threat research team has found the North Korean 'SharpTongue' group, which appears to be part of, or related to, the Kimsuky advanced persistent threat group, deploying malware called SHARPEXT that doesn't need your Gmail login credentials at all.

Instead, it "directly inspects and exfiltrates data" from a Gmail account as the victim browses it. This quickly evolving threat, Volexity says it is already on version 3.0 according to the malware's internal versioning, can steal email from both Gmail and AOL webmail accounts, and works across three browsers: Google Chrome, Microsoft Edge, and a South Korean client called Whale.

CISA says Kimsuky hackers 'most likely tasked by North Korean regime'

The U.S. Cybersecurity & Infrastructure Security Agency, CISA, reports that Kimsuky has been operating since 2012, and is "most likely tasked by the North Korean regime with a global intelligence gathering mission."

While CISA sees Kimsuky most often targeting individuals and organizations in South Korea, Japan, and the U. S., Volexity says that the SharpTongue group has frequently been seen targeting South Korea, the U. S. and Europe. The common denominator between them is that the victims often " work on topics involving North Korea, nuclear issues, weapons systems, and other matters of strategic interest to North Korea."

What's different about the SHARPEXT threat to Gmail?

The report says that SHARPEXT differs from previous browser extensions deployed by these hacking espionage groups in that it doesn't attempt to grab login credentials but bypasses the need for these and can grab email data as the user reads it.

The good news is that your system needs to be compromised by some means before this malicious extension can be deployed. Unfortunately, we know all too well that system compromise is not as difficult as it should be.

Once a system has been compromised by phishing, malware, unpatched vulnerabilities, whatever, the threat actors can install the extension using a malicious VBS script that replaces the system preference files. Once that's done and the extension runs quietly in the background, it is tough to detect. The user logs in to their Gmail account from their normal browser on the expected system.

SHARPEXT reads Gmail emails silently without triggering Google unusual usage protections

There is nothing to alert Google and the user that someone has logged into Gmail from a different browser, machine, or location. Bypassing this protection is crucial as it means the threat actors can remain truly persistent, reading all the received and sent emails as if they were the user themselves.

To detect and investigate a SHARPEXT attack, Volexity recommends enabling and analyzing PowerShell Script-Block logging as PowerShell plays a key role in the setup and installation of the malware. Review installed extensions regularly, especially looking for ones you don't recognize or are not available from the Chrome Web Store.

That said, the average user should not worry too much as this group's victims will be specifically targeted. Of course, if you work in a field that may interest them, then you are in the crosshairs.

A Google spokesperson provided me with the following statement: "The extension in question is not in the Chrome store, and this report does not identify an exploit in Gmail. It speaks to a scenario where a system needs to already be compromised—by spear phishing or social engineering–in order for the malicious extension to be deployed. Enabling anti-malware services and using security hardened operating systems like ChromeOS are best practices to prevent this and similar types of attacks."

A SHARPEXT threat assessment by former military and law enforcement intelligence analyst

I also spoke to Ian Thornton-Trump, CISO at threat intelligence specialists Cyjax. A former criminal intelligence analyst with the Royal Canadian Mounted Police and having also served with the Canadian Forces' Military Intelligence Branch, he's well placed to assess this kind of suspected nation-state aligned threat.

"This is interesting to me for a couple of reasons. Firstly, I think North Korea is trying to be more proactive and threatening as the world's attention is far more focused on Russian and China's geopolitical ambitions. North Korea is not getting the attention it used to. The threat of nukes from North Korea, missile tests, and cyberattacks has been reduced to slightly more than background noise with the focus on the pandemic, the war in Europe, and global climate change," Thornton-Trump says.

While confirming that malicious browser extensions are nothing new regarding threat actors aligned to North Korean interests, Thornton-Trump confessed to being somewhat surprised that the threat focus wasn't ransomware or cryptocurrency wallets. "North Korea remains an international pariah state when it comes to accessing financial services," he says, "and has been surviving on effective exploitation of cryptocurrency exchanges and wallets to prop up its economy."

Directly targeting Gmail content is likely espionage oriented

Regarding SHARPEXT, Thornton-Trump agrees that directly targeting Gmail (and AOL webmail) contents displayed in a web browser is far more espionage oriented. "This could be perceived as a change in tactics," he told me, "but email attacks have broad impact and are perfect for lateral movement into third-party apps as well as access to sensitive information."

Once the host is compromised, he added that it would be interesting to know if the threat actor went into listen-only mode via exfiltration or pivoted into active exploitation.

"Remarkably, the malware is delivered and installed by PowerShell, something all too typical, and you would think that by now, the built-in protections to the Microsoft Operating System, third-party extended detection and response (XDR), and endpoint detection and response (EDR), along with browser malware protection in the Windows version of Chrome," he concludes, "would easily prevent these invoke- PowerShell attacks. Especially on workstations where you would think PowerShell activities would be rare for most victim organization's users."

22.German semiconductor giant Semikron says hackers encrypted its network

by Carly Page
https://techcrunch.com/2022/08/03/semikron-hackers-encrypted-electric-vehicles/

Semikron, a German manufacturer that produces semiconductors for electric vehicles and industrial automation systems, has confirmed it has fallen victim to a cyberattack that has resulted in data encryption.

"Semikron is already in the process of dealing with the situation so that workflows and all related processes can continue without disruption for both employees and customers as soon as possible," a Semikron spokesperson told TechCrunch.

Semikron declined to disclose the nature of the cyberattack, but all signs point to ransomware. The semiconductor maker said in a statement that hackers claim to have "exfiltrated data from our system," adding that the incident has led to a "partial encryption of our IT systems and files." This suggests the malicious actor behind the attack has used the double extortion ransomware tactic, whereby cybercriminals exfiltrate a victim's sensitive data in addition to encrypting it.

The Nuremberg-based company, which claims to power 35% of the wind turbines installed globally each year, declined to say who was behind the attack, nor whether it received a ransom demand. However, Bleeping Computer reports that Semikron was the victim of the LV ransomware, with the hackers apparently stealing 2 terabytes of documents.

LV ransomware has been in operation since at least 2020 and uses a modified variant of REvil ransomware, according to cybersecurity company Secureworks. According to the group's dark web blog, which doesn't yet list Semikron as a victim, the gang targets companies that allegedly do not meet data protection obligations.

"They rejected to fix their mistakes, they rejected to protect this data in the case when they could and had to protect it," its dark web blog states. "These companies preferred to sell their private information, their employees' and customers' personal data."

It's unclear what data was exfiltrated from Semikron's systems, and the company declined to say how many customers and employees are potentially impacted. Semikron has more than 3,000 employees in 24 offices and eight production sites worldwide across Germany, Brazil, China, France, India, Italy, Slovakia and the United States.

"With the support of external cyber security and forensic experts, we are investigating the incident," Semikron added. "At the same time, we are working to restore the ability to work in order to minimize the disruption to our employees, customers and partners and to ensure the security of our IT systems as best as possible."

23.Post-quantum crypto cracked in an hour with one core of an ancient Xeon

by Laura Dobberstein
https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked/?utm_source=daily&utm_medium=newsletter&utm_content=top-article

One of the four encryption algorithms America's National Institute of Standards and Technology (NIST) recommended as likely to resist decryption by quantum computers has had holes kicked in it by researchers using a single core of a regular Intel Xeon CPU, released in 2013.

The Supersingular Isogeny Key Encapsulation (SIKE) algorithm was chosen by NIST just last month as a candidate for standardization, meaning it advanced to an extra round of testing en route to adoption.

Within SIKE lies a public key encryption algorithm and a key encapsulated mechanism, each instantiated with four parameter sets: SIKEp434, SIKEp503, SIKEp610 and SIKEp751.

Microsoft – whose research team played a role in the algorithm's development along with multiple universities, Amazon, Infosec Global and Texas Instruments – set up a $50,000 bounty for anyone who could crack it.

Belgian boffins Wouter Castryck and Thomas Decru claim to have done just that, using some good ol' non-quantum x86 silicon.

"Ran on a single core, the appended Magma code breaks the Microsoft SIKE challenges $IKEp182 and $IKEp217 in about 4 minutes and 6 minutes, respectively. A run on the SIKEp434 parameters, previously believed to meet NIST's quantum security level 1, took about 62 minutes, again on a single core," wrote Castryck and Decru, of Katholieke Universiteit Leuven (KU Leuven) in a a preliminary article [PDF] announcing their discovery.

The authors made their code public, as well as the details of their processor: an Intel Xeon CPU E5-2630v2 at 2.60GHz. That bit of kit was launched in Q3 2013, used Intel's Ivy Bridge architecture and a 22nm manufacturing process. The chip offered six cores – not that five of them were in any way encumbered by this challenge.

- Actual quantum computers don't exist yet. The cryptography to defeat them may already be here
- Warning: China planning to swipe a bunch of data soon so quantum computers can decrypt it later
- IBM puts NIST's quantum-resistant crypto to work in Z16 mainframe
- NSA: We 'don't know when or even if' a quantum computer will ever be able to break today's public-key encryption

Quantum-resistant encryption research is a hot topic because it is felt that quantum computers are almost cer-

tain to become prevalent and sufficiently powerful to crack existing encryption algorithms. It is therefore prudent to prepare crypto that can survive future attacks, so that data encrypted today remains safe tomorrow, and digital communications can remain secure.

Thus, bounties for testing its limits abound.

Microsoft described the algorithm as using arithmetic operations on elliptic curves defined over finite fields and compute maps, also called isogenies, between the curves.

Finding such an isogeny was thought to be sufficiently difficult to provide reasonable security – a belief now shattered by nine-year-old tech.

Alongside the vintage processor, Castryck and Decru used a key recovery attack on the Supersingular Isogeny Diffie–Hellman key exchange protocol (SIDH) that was based on Ernst Kani's "glue-and-split" theorem.

"The attack exploits the fact that SIDH has auxiliary points and that the degree of the secret isogeny is known. The auxiliary points in SIDH have always been an annoyance and a potential weakness, and they have been exploited for fault attacks, the GPST adaptive attack, torsion point attacks, etc." argued University of Auckland mathematician Stephen Galbraith in his cryptography blog.

The math gets cerebral, and Galbraith suggests if you really want to understand it, you need to study Richelot isogenies and abelian surfaces.

Damn. Another missed opportunity during lockdown.

But we digress. For those who already have a rich background in elliptic curve cryptography and want a quick immersion, there are several Twitter threads that analyze the achievement at greater depth.

Some professionals in the arena propose that not all is lost with SIKE.

SIKE co-creator David Jao reportedly believes the NIST submitted version of SIKE used a single step to generate the key, and a possible more resilient variant could be constructed with two steps.

That possibility lies still in a yet undiscovered portion of the intersection of mathematics and computer science. In the meantime, cryptography experts are shaken.

"There is no doubt that this result will reduce confidence in isogenies. The sudden appearance of an attack this powerful shows that the field is not yet mature," commented Galbraith.

Security researcher Kenneth White tweeted his awe and noted "In 10-20 yrs (or 50, or never) we *might* have practical quantum computers, so let's roll out replacement PQ crypto now. Which could be trivially broken today, on a laptop."

But as Kevin Reed, CISO of cybersecurity firm Acronis, put it in a LinkedIn post: "It's still better than if it was discovered after it is standardized."

24.Post-quantum encryption contender is taken out by single-core PC and 1 hour

by Dan Goodin
https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-con-

tender-is-koed-in-nist-smack-down/?amp=1#amp_tf=From%20%251%24s&aoh=16595287152515&csi=0&referrer=https%3A%2F%2Fwww.google.com

In the US government's ongoing campaign to protect data in the age of quantum computers, a new and powerful attack that used a single traditional computer to completely break a fourth-round candidate highlights the risks involved in standardizing the next generation of encryption algorithms.

Last month, the US Department of Commerce's National Institute of Standards and Technology, or NIST, selected four post-quantum computing encryption algorithms to replace algorithms like RSA, Diffie-Hellman, and elliptic curve Diffie-Hellman, which are unable to withstand attacks from a quantum computer.

In the same move, NIST advanced four additional algorithms as potential replacements pending further testing in hopes one or more of them may also be suitable encryption alternatives in a post-quantum world. The new attack breaks SIKE, which is one of the latter four additional algorithms. The attack has no impact on the four PQC algorithms selected by NIST as approved standards, all of which rely on completely different mathematical techniques than SIKE.

Getting totally SIKEd

SIKE—short for Supersingular Isogeny Key Encapsulation—is now likely out of the running thanks to research that was published over the weekend by researchers from the Computer Security and Industrial Cryptography group at KU Leuven. The paper, titled An Efficient Key Recovery Attack on SIDH (Preliminary Version), described a technique that uses complex mathematics and a single traditional PC to recover the encryption keys protecting the SIKE-protected transactions. The entire process requires only about an hour's time. The feat makes the researchers, Wouter Castryck and Thomas Decru eligible for a $50,000 reward from Microsoft.

"The newly uncovered weakness is clearly a major blow to SIKE," David Jao, a professor at the University of Waterloo and co-inventor of SIKE, wrote in an email. "The attack is really unexpected."

The advent of public key encryption in the 1970s was a major breakthrough because it allowed parties who had never met to securely trade encrypted material that couldn't be broken by an adversary. Public key encryption relies on asymmetric keys, with one private key used to decrypt messages and a separate public key for encrypting. Users make their public key widely available. As long as their private key remains secret, the scheme remains secure.

In practice, public key cryptography can often be unwieldy, so many systems rely on key encapsulation mechanisms, which allow parties who have never met before to jointly agree on a symmetric key over a public medium such as the Internet. In contrast to symmetric-key algorithms, key encapsulation mechanisms in use today are easily broken by quantum computers. SIKE, before the new attack, was thought to avoid such vulnerabilities by using a complex mathematical construction known as a supersingular isogeny graph.

The cornerstone of SIKE is a protocol called SIDH, short for Supersingular Isogeny Diffie-Hellman. The research paper published over the weekend shows how SIDH is vulnerable to a theorem known as "glue-and-split" developed by mathematician Ernst Kani in 1997, as well as tools devised by fellow mathematicians Everett W. Howe, Franck Leprévost, and Bjorn Poonen in 2000. The new technique builds on what's known as the "GPST adaptive attack," described in a 2016 paper. The math behind the latest attack is guaranteed to be impenetrable to most non-mathematicians. Here's about as close as you're going to get: "The attack exploits the fact that SIDH has auxiliary points and that the degree of the secret isogeny is known," Steven Galbraith, a University of Auckland mathematics professor and the "G" in the GPST adaptive attack, explained in a short writeup on the new attack. "The auxiliary points in SIDH have always been an annoyance and a potential weakness, and they have

been exploited for fault attack, torsion point attacks, the GPST adaptive attacks, etc.

He continued:

More important than understanding the math, Jonathan Katz, an IEEE Member and professor in the department of computer science at the University of Maryland, wrote in an email: "the attack is entirely classical, and does not require quantum computers at all."

Lessons learned

SIKE is the second NIST-designated PQC candidate to be invalidated this year. In February, IBM post-doc researcher Ward Beullens published research that broke Rainbow, a cryptographic signature scheme with its security, according to Cryptomathic, "relying on the hardness of the problem of solving a large system of multivariate quadratic equations over a finite field."

NIST's PQC replacement campaign has been running for five years. Here's a brief history:

- 1st round (2017)—69 candidates
- 2nd round (2019)—26 surviving candidates
- 3rd round (2020)—7 finalists, 8 alternates
- 4th round (2022)—3 finalists and 1 alternate selected as standards. SIKE and three additional alternates advanced to a fourth round.

Rainbow fell during Round 3. SIKE had made it until Round 4.

Katz continued "It is perhaps a bit concerning that this is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (The earlier example was Rainbow, which was broken in February.) Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward."

I asked Jao, the SIKE co-inventor, why the weakness had come to light only now, in a relatively later stage of its development. His answer was insightful. He said: "It's true that the attack uses mathematics which was published in the 1990s and 2000s. In a sense, the attack doesn't require new mathematics; it could have been noticed at any time. One unexpected facet of the attack is that it uses genus 2 curves to attack elliptic curves (which are genus 1 curves). A connection between the two types of curves is quite unexpected. To give an example

illustrating what I mean, for decades people have been trying to attack regular elliptic curve cryptography, including some who have tried using approaches based on genus 2 curves. None of these attempts has succeeded. So for this attempt to succeed in the realm of isogenies is an unexpected development.

In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should. So sometimes all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems. That is what happened here."

The version of SIKE submitted to NIST used a single step to generate the key. A possible variant of SIKE could be constructed to take two steps. Jao said that it's possible that this latter variant might not be susceptible to the math causing this breakage. For now, though, SIKE is dead, at least in the current running. The schedule for the remaining three candidates is currently unknown.

25.The Million Dollar Problem That Could Break Cryptography

by Leo Gu
https://scitechdaily.com/the-million-dollar-problem-that-could-break-cryptography/amp/#amp_tf=From%20%251%24s&aoh=16595285917147&csi=1&referrer=https%3A%2F%2Fwww.google.com

The P vs NP problem is one of the most difficult problems in theoretical computer science.

P versus NP

Usually, you can verify a solution to a problem. Whether it's using multiplication for division or plugging the answer in for a variable, math teachers tell you to check your work using your answer in every school math class.

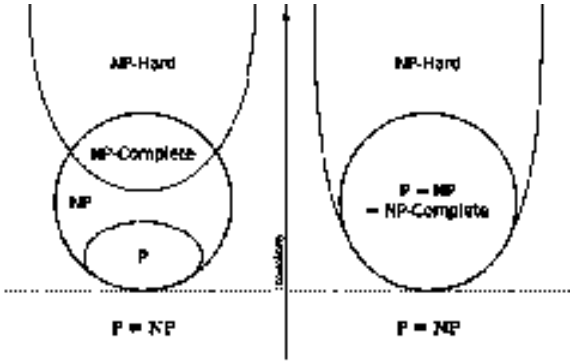
But let's say you can verify a solution easily, is it just as easy to solve for that solution?

This is the P versus NP problem, a Millenium Prize Problem where the solver will receive a million dollars if valid proof is provided.

What is P versus NP?

In computer science, the efficiency of algorithms is very important. Most algorithms are believed to be "fast" if solvable in a standard called polynomial time. Polynomial time is when a problem is solvable in steps scaled by a factor of a polynomial given the complexity of input. So let's say the complexity of input is some number n, a polynomial time algorithm will be able to solve a problem in n^k steps.

Essentially, P vs NP is asking the question: Are problems that can have solutions verified in polynomial time,



also have their answers solved in polynomial time?

NP-Completeness

One of the most prominent subproblems is NP-complete problems. NP-complete problems are ones that can be verified quickly and that can be used to simulate every other NP-complete problem. Therefore, solving one of these problems in polynomial time is a major boost to solving P vs NP. Some of these problems include games like Battleship and the optimal solution to an $N \times N \times N$ Rubik's Cube but also include famous theoretical questions like the traveling salesman problem. If a solution for any of these is found, a general solution for NP-complete problems can also be found.

Impact

If P is proven to equal NP, there could be serious consequences and benefits. Cybersecurity would be a huge issue as public-key cryptography would be upended and many ciphers could be cracked. However, there would also be improvements in research of protein structure prediction and overall computing because of better integer programming and the solving of the traveling salesman problem.

If P is proven to not equal NP, there would be nearly no drawbacks and benefits. Researchers would then focus less on a general solution to all NP-complete problems which would not really change much. Closing

P vs NP is a critical unsolved problem in computer science that could have drastic effects. Though the major consensus is that P is not equal to NP, any widely accepted proof would rattle the scientific world.

References:

1. "The P vs NP Problem" by Stephen Cook, 2001, claymath.org

2. "Computers and Intractability: A guide to the Theory of NP-Completeness" by Michael Garey, David S Johnson, 1979, ISBN 0-7167-1045-5

26.What is a QPU and how will it drive quantum computing?

by Rick Merritt and Yunchao Liu
https://it-online.co.za/2022/08/01/what-is-a-qpu-and-how-will-it-drive-quantum-computing/

Just as GPUs and DPUs enable accelerated computing today, they're also helping a new kind of chip, the QPU,

boot up the promise of quantum computing.

In your hand, a quantum processing unit might look and feel very similar to a graphics or a data processing unit. They're all typically chips, or modules with multiple chips, but under the hood the QPU is a very different beast.

So what's a QPU?

A QPU, aka a quantum processor, is the brain of a quantum computer that uses the behaviour of particles like electrons or photons to make certain kinds of calculations much faster than processors in today's computers.

QPUs rely on behaviours like superposition, the ability of a particle to be in many states at once, described in the relatively new branch of physics called quantum mechanics.

By contrast, CPUs, GPUs and DPUs all apply principles of classical physics to electrical currents. That's why today's systems are called classical computers.

QPUs could advance cryptography, quantum simulations and machine learning and solve thorny optimisation problems.

QPUS	GPUS
Quantum processing units	Graphics processing units
Relies on quantum physics	Relies on classical physics
Uses qubits that can be more than 0 and 1	Uses bits that are either 0 or 1
Uses states of subatomic particles	Uses electricity switched in transistors
Great for cryptography and simulating quantum effects	Great for HPC, AI and classical simulations

How does a quantum processor work?

CPUs and GPUs calculate in bits, on/off states of electrical current that represent zeros or ones. By contrast, QPUs get their unique powers by calculating in qubits — quantum bits that can represent many different quantum states.

A qubit is an abstraction that computer scientists use to express data based on the quantum state of a particle in a QPU. Like the hands on a clock, qubits point to quantum states that are like points in a sphere of possibilities.

The power of a QPU is often described by the number of qubits it contains. Researchers are developing additional ways to test and measure the overall performance of a QPU.

Many ways to make a qubit

Corporate and academic researchers are using a wide variety of techniques to create the qubits inside a QPU.

The most popular approach these days is called a superconducting qubit. It's basically made from one or more tiny metallic sandwiches called Josephson junctions, where electrons tunnel through an insulating layer between two superconducting materials.

The current state of the art creates more than 100 of these junctions into a single QPU. Quantum computers using this approach isolate the electrons by cooling them to temperatures near absolute zero with powerful refrigerators that look like high-tech chandeliers.

A qubit of light

Some companies use photons rather than electrons to form qubits in their quantum processors. These QPUs don't require expensive, power-hungry refrigerators, but they need sophisticated lasers and beam splitters to manage the photons.

Researchers are using and inventing other ways to create and connect qubits inside QPUs. For example, some use an analogue process called quantum annealing, but systems using these QPUs have limited applications.

It's early days for quantum computers, so it's not yet clear what sorts of qubits in what kinds of QPUs will be widely used.

Simple chips, exotic systems

Theoretically, QPUs may require less power and generate less heat than classical processors. However, the quantum computers they plug into can be somewhat power hungry and expensive.

That's because quantum systems typically require specialised electronic or optical control subsystems to precisely manipulate particles. And most require vacuum enclosures, electromagnetic shielding or sophisticated refrigerators to create the right environment for the particles.

That's one reason why quantum computers are expected to live mainly in supercomputing centers and large data centres.

QPUs do cool stuff

Thanks to the complex science and technology, researchers expect the QPUs inside quantum computers will deliver amazing results. They are especially excited about four promising possibilities.

First, they could take computer security to a whole new level.

Quantum processors can factor enormous numbers quickly, a core function in cryptography. That means they could break today's security protocols, but they can also create new, much more powerful ones.

In addition, QPUs are ideally suited to simulating the quantum mechanics of how stuff works at the atomic level. That could enable fundamental advances in chemistry and materials science, starting domino effects in everything from the design of lighter airplanes to more effective drugs.

Researchers also hope quantum processors will solve optimization problems classical computers can't handle in fields like finance and logistics. And finally, they may even advance machine learning.

So when will QPUs be available?

For quantum researchers, QPUs can't come soon enough. But challenges span the gamut.

On the hardware level, QPUs are not yet powerful or dependable enough to tackle most real-world jobs. However, early QPUs – and GPUs simulating them with software like Nvidia cuQuantum — are beginning to show results that help researchers, especially in projects exploring how to build better QPUs and develop quantum algorithms.

Researchers are using prototype systems available through several companies like Amazon, IBM, IonQ, Rigetti, Xanadu and more. Governments around the world are beginning to see the promise of the technology, so they're making significant investments to build ever larger and more ambitious systems.

How do you program a quantum processor?

Software for quantum computing is still in its infancy.

Much of it looks like the kind of assembly-language code programmers had to slog through in the early days of classical computers. That's why developers have to understand the details of the underlying quantum hardware to get their programs running.

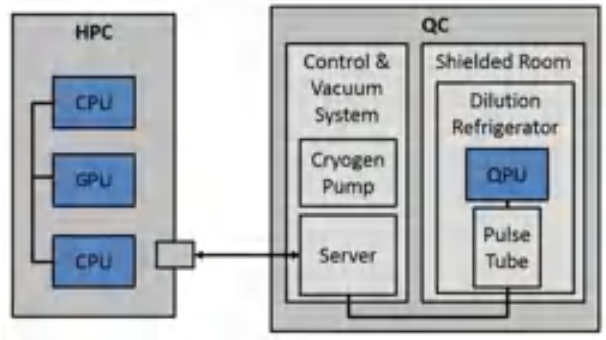
But here, too, there are real signs of progress toward the holy grail — a single software environment that will work across any supercomputer, a sort of quantum OS.

Several early projects are in the works. All struggle with the limitations of the current hardware; some are hampered by the limits of the companies developing the code.

For example, some companies have deep expertise in enterprise computing but lack experience in the kind of high-performance environments where much of the scientific and technical work in quantum computing will be done. Others lack expertise in AI, which has synergies with quantum computing.

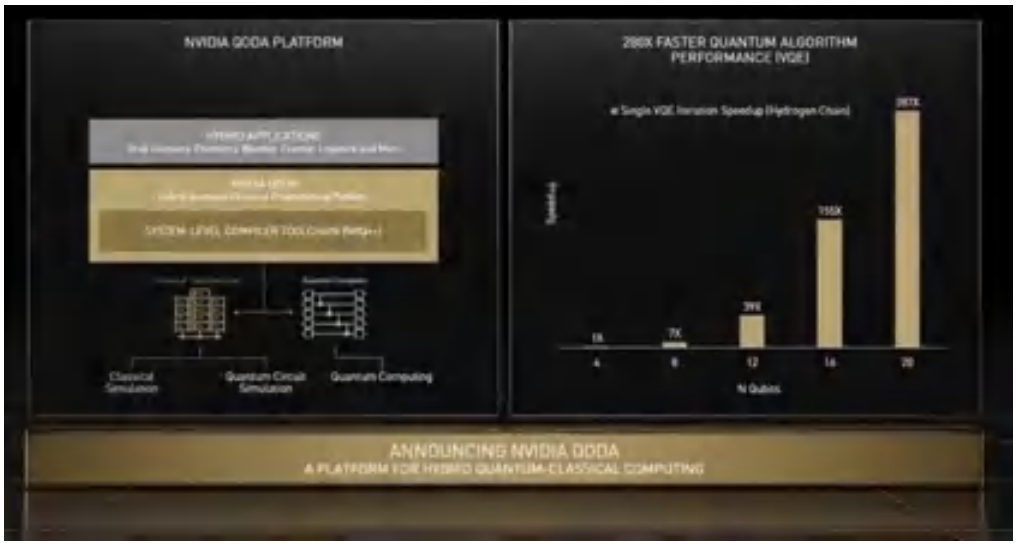
Enter hybrid quantum systems

The research community widely agrees that for the foreseeable future, classical and quantum computers will



work in tandem. So, software needs to run well across QPUs, CPU and GPUs, too.
To drive quantum computing forward, Nvidia recently announced the Nvidia Quantum Optimized Device Architecture (QODA), an open platform for programming hybrid quantum systems.

QODA includes a high-level language that's concise and expressive so it's powerful and easy to use. With QODA, developers can write programs that run on QPUs in quantum computers and GPUs simulating QPUs in classical



systems.
QODA will support every kind of quantum computer and every sort of QPU.

At its launch, quantum system and software providers including Pasqal, Xanadu, QC Ware and Zapata expressed support for QODA. Users include major supercomputing centers in the US and Europe.

QODA builds on NVIDIA's extensive expertise in CUDA software, which accelerates HPC and AI workloads for scientific, technical and enterprise users.

With a beta release of QODA expected before the end of the year, the outlook for QPUs in 2023 and beyond is bright.

