Crypto News

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

February 01, 2024

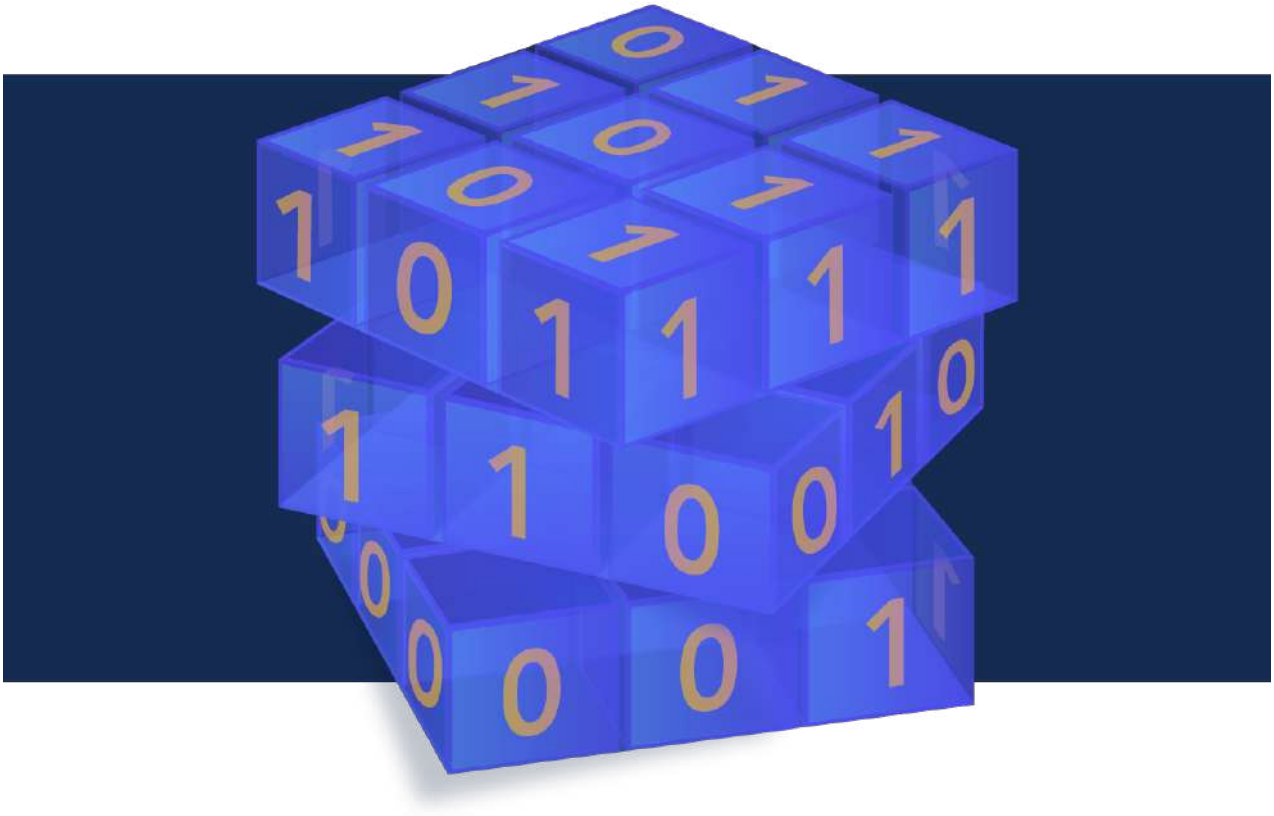


TABLE OF CONTENTS

1.FRENCH NATIONAL QUANTUM UPDATE — JANUARY 2024 5

2.NIST COLLABORATES WITH KOREA RESEARCH INSTITUTE OF STANDARDS AND SCIENCE ON QUANTUM COMPUTING 7

3.QUSECURE CONTRIBUTES TO WHITE HOUSE QUANTUM SECURITY ROUNDTABLE ADDRESSING THE POST-QUANTUM CYBERSECURITY THREAT 7

4.KOREA QUANTUM COMPUTING AND IBM COLLABORATE TO BRING IBM WATSONX AND QUANTUM COMPUTING TO KOREA 9

5.CISCO ANNOUNCES NEW QUANTUM NETWORKING COLLABORATION WITH UK STARTUP 10

6.CRYPTOGRAPHIC STORAGE IS A SECURE WAY TO STORE DATA USING ENCRYPTION AND OTHER SECURITY MEASURES. 11

7.IS Q-DAY — THE DAY QUANTUM COMPUTING HACKS EVERYTHING — APPROACHING? 12

8.WHAT IS THE QUANTUM THREAT AND WHAT HAS SIMPLE MATHS GOT TO DO WITH PROTECTING GLOBAL SECURITY? 16

9.DORA AND YOUR QUANTUM-SAFE CRYPTOGRAPHY MIGRATION 19

10.A DETAILED JOURNEY WITH OLIVIA LANES EXPLORING THE IBM QUANTUM LAB, REVEALS THE INTRICACIES OF QUANTUM COMPUTING 23

11.CHINESE SCIENTISTS REALIZE CROSSTALK-AVOIDED QUANTUM NETWORK NODE 24

12.CRYPTOGRAPHERS JUST GOT CLOSER TO ENABLING FULLY PRIVATE INTERNET SEARCHES 24

13.PREPARING FOR POST-QUANTUM CRYPTOGRAPHY: TRUST IS THE KEY 27

14.QUANTUM-SECURE ONLINE SHOPPING COMES A STEP CLOSER 29

15.CYBER-ATTACKS AGAINST AMERICANS AT ALL TIME HIGH OVER PAST TWO YEARS 30

16.QUANTUM COMPUTING AND ITS IMPACT ON CORPORATE SECURITY AND PRIVACY COMPLIANCE 32

17.INDIA'S EMERGENCE MAKES IT A CRITICAL PARTNER FOR THE WESTERN QUANTUM ECOSYSTEM 33

18.SUMMARY OF NATO'S QUANTUM TECHNOLOGIES STRATEGY 36

19.ENSILICA ADDS POST QUANTUM CRYPTOGRAPHY SUPPORT TO ESI-CRYPTO IP LIBRARY 39

20.ENCRYPTED MOBILES WITH EXCLUSIVE OPERATING SYSTEM — HOW ARMY IS MOVING TOWARDS SECURE COMMUNICATION 40

21.ENTRUST INTRODUCES FIRST COMMERCIALLY AVAILABLE "POST QUANTUM READY" PKI PLATFORM 41

22.CHINA CLAIMS IT HAS CRACKED APPLE AIRDROP'S ENCRYPTION TO IDENTIFY SENDERS 42

23.QUERA COMPUTING ROADMAP FOR ADVANCED ERROR-CORRECTED QUANTUM COMPUTERS, PIONEERING THE NEXT FRONTIER IN QUANTUM INNOVATION 43

24.TAIWAN EYES 2027 FOR FIRST LOCAL QUANTUM COMPUTER 45

25.KYBERSLASH ATTACKS PUT QUANTUM ENCRYPTION PROJECTS AT RISK 46

26.THE NEED FOR POST-QUANTUM CRYPTOGRAPHY IN THE QUANTUM DECADE 48

27.QUANTUM COMPUTING IS TAKING ON ITS BIGGEST CHALLENGE: NOISE 49

28.SK, THALES COLLABORATE ON 5G POST-QUANTUM CRYPTOGRAPHY 53

29.SIDE-CHANNEL ATTACK PROTECTION FOR QUANTUM SAFE CRYPTOGRAPHY 53

30.UAE, SAUDI ARABIA, AND QATAR SPEARHEADING QUANTUM COMPUTING DEVELOPMENT IN THE MIDDLE EAST 55

31.HOW CAN SMES PREPARE FOR THE QUANTUM COMPUTING ERA? 57

Editorial

It's February and I'm excited to be back! Of course I have to start by sharing my thoughts about one of my top three favourite topics to talk about – quantum computing. Many of us know the importance of quantum computers and how they will impact our lives. However, there's always that pesky problem of "noise" to deal with. Some thought the problem of noise may be insurmountable, but there were others who saw the challenge of noise as their calling. There are now several solutions, with one of them being a set of solutions that are used in a series, to help mitigate the effects of noise. Article 27 walks us through how we got here today and what the set of solutions are as well as other solutions including, but not limited to, QEC aka Quantum Error Correction. With these advancements, we are well on our way to a quantum computer showing a quantum advantage sooner rather than later.

Now let's move on to another one of my favourite topics – cybersecurity. It is well known in the cybersecurity community that the infrastructure of many nations, including the United States, is vulnerable to attack by nation states and other adversaries. Just a few days ago, FBI Director Christopher Wray warned against the threat certain nations play to the safety of the American people at the national level. Often overlooked is the impact of cyber attacks at the local government level. Article 15 outlines the threat at the local level specifically related to education and research. Having had the privilege to work in a variety of industries including local government, it is safe to say that increased government spending is needed to secure our sensitive data and our futures.

Don't miss out on reading about my third favourite topic, cryptography (which is a large player in quantum computing and cybersecurity so it makes sense it's in the top three for me), which is sprinkled throughout this newsletter. Until next time, happy reading!

The Crypto News editorial is authored by the co-Chair of the Quantum-Safe Security-Working Group (QSS WG) of the Cloud Security Alliance (CSA), Mehak Kalsi, MS, CISSP, CISA, CMMC-CCP and it is compiled by Dhananjoy Dey. Both are active members of the CSA 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.French National Quantum Update — January 2024

by Matt Swayne
https://thequantuminsider.com/2024/01/31/french-national-quantum-update-january-2024/

Executive Summary

January 2024 may go down in the record books as one of the most exciting, one of the most productive months in the history of the French quantum ecosystem's young history. The French quantum ecosystem. Alice & Bob released information on error-correction research that suggests the company could be on the cusp of practical quantum computing.

French policymakers, scientists and entrepreneurs are moving into the new year with a deepening commitment to quantum. In this first month of 2024, we can see the interlocking parts of the French quantum ecosystem are already forging ahead at a rapid pace. On the policy front, global events, such as Davos, gave France the spotlight to reveal their quantum and deep tech aspirations.

POLICY

MACRON AT DAVOS: INCLUDES QUANTUM IN A STRATEGIC ECONOMIC BLUEPRINT FOR FRANCE'S AND EUROPE'S FUTURE French President Emmanuel Macron presented a comprehensive vision for the future of France and Europe at the World Economic Forum (WEF) in Davos on Wednesday, emphasising economic reforms, environmental sustainability, and the strengthening of European sovereignty.

Macron stressed the need for more investment in various sectors, stating, "Quantum, clean, green tech or even the defence sector requires much more money. We need an investment strategy with two drivers."

FRENCH QUANTUM SECTOR CALLS FOR MORE EU FUNDING technologies, according to founders and strategists working within the quantum field in France. Quantum computing is based on the theoretical promise that quantum calculation capacities can immensely reduce the calculation speed of highly complex problems, bringing the time down from years to hours or even minutes.

Business

ACCELERATING INNOVATION WITH QPUS Quantum computing is a promising solution that can exponentially increase the speed of solving various problems. Quantum Processing Units (QPUs) have progressed significantly in recent years, developing from lab experiments to industrial products. They have reached the first level of maturity and can now be integrated into High-Performance Computing (HPC) centers.

GLOBAL FINANCIAL SYSTEM FACES PROSPECT OF QUANTUM COMPUTING THREATS The potential threats posed by advances in quantum computing to public-key cryptography (PKC) protocols widely used in the global financial system appear set to draw increased attention from governments and regulators amid intensifying efforts to mitigate the risk, says Fitch Ratings. Interoperability with legacy cryptography systems could present particular issues for financial institutions, and has been a focus of the BIS's Project Leap, a pilot scheme run with the French and German central banks aiming to counter quantum

computing threats to financial-system data security.

PASQAL JOINS FORCES WITH MILA TO ENHANCE GENERATIVE MODELING IN QUANTUM AI Mila is proud to welcome PASQAL, a global leader in neutral atom quantum computing, to its partner community. This collaboration will be a first exploratory step towards enhancing generative modeling with quantum computing benchmarking and coupling with tensor networks.

PASQAL WELCOMES ROBERTO MAURO AS GENERAL MANAGER TO SPEARHEAD OPERATIONS IN SOUTH KOREA PASQAL, a global leader in neutral atom quantum computing, proudly announces the appointment of Roberto Mauro as General Manager for South Korea, marking a significant step in its global expansion. PASQAL is now present in 6 countries, France, United States, Netherlands, Canada, Saudi Arabia and South Korea.

THALES AND QUANTINUUM LAUNCH STARTER KIT TO PREPARE ENTERPRISES FOR POST-QUANTUM CRYPTOGRAPHY CHANGES AHEAD Thales, the leading global technology and security provider, today announced the launch of its PQC Starter Kit in collaboration with Quantinuum. This first-of-its-kind offering helps enterprises prepare for Post-Quantum Cryptography (PQC). The kit provides a trusted environment for businesses to test quantum-hardened PQC-ready encryption keys and understand the implications that quantum computing will have on the security of their infrastructure.

GEN AI AND QUANTUM TO DESIGN NEW DRUGS: PARIS-BASED AQEMIA COMPLETES €60M SERIES A Paris-based biotech Aqemia, which uses AI to fast-track drug discovery and design, has raised a €30m extension to its Series A, bringing total funding for the round to an all-equity €60m. The startup raised a first €30m in 2022 led by French VC Eurazeo and public bank Bpifrance, with historical investor Elaia also participating. The latest extension, led by French growth investor Wendel Growth, saw all three of Aqemia's previous investors return.

QUBIT PHARMACEUTICALS ADVANCES CANCER RESEARCH WITH HPC AND AI-POWERED DRUG DISCOVERY IN COLLABORATION WITH FRENCH RESEARCH INSTITUTIONS Qubit Pharmaceuticals, a company specializing in the discovery of new drug candidates using simulation and AI accelerated by hybrid HPC and quantum computing, and Institut Curie, France's leading center in the fight against cancer, have announced their collaboration in the search for new therapeutic avenues to treat cancer. The project will be carried out in partnership with the Laboratoire de Microbiologie Fondamentale et Pathogénicité at the University of Bordeaux.

Research

ALICE & BOB-LED RESEARCH SHOWS NOVEL APPROACH TO ERROR CORRECTION COULD REDUCE NUMBER OF QUBITS FOR USEFUL QUANTUM COMPUTING Alice & Bob, a leading hardware developer in the race to fault tolerant quantum computers, in collaboration with the research institute Inria, today announced a new quantum error correction architecture – low-density parity-check (LDPC) codes on cat qubits – to reduce hardware requirements for useful quantum computers.

FRANCE'S MICHEL DEVORET HELPED LEAD YALE'S QUANTUM COMPUTING JOURNEY Yale's quest to build the world's first, fully useful quantum computer is also the story of a small-town kid's obsession with short-wave radios, a Parisian's fond boyhood memories of America, and a high school student from the New York suburbs who soaked up Saturday morning science programs at Yale's Becton Center. It is the story of three physicists — Robert Schoelkopf, Michel Devoret, and Steven Girvin — who converged at Yale and helped shape the way scientists worldwide approach the emerging field of quantum computing.

Education and Events

LYON WINTER SCHOOL OF QUANTUM TECHNOLOGIES 2024 The Lyon Winter School of Quantum

Technologies is a week-long program that introduces students and post-docs to the fundamentals of quantum technologies. This year's session was held at Ecole Normale Supérieure de Lyon and includes evaluations through report writing on selected articles. Funding is provided by the program **France 2030**.

2.NIST Collaborates with Korea Research Institute of Standards and Science on Quantum Computing

https://www.hpcwire.com/off-the-wire/nist-collaborates-with-korea-research-institute-of-standards-and-science-on-quantum-computing/

On January 29, 2024, representatives of NIST and the Republic of Korea's government metrology agency – the Korea Research Institute of Standards and Science (KRISS)– signed an amendment to an existing memorandum of understanding to include cooperation on research and development (R&D) related to Precision Metrology for Quantum Computing.

The signing occurred at NIST's Boulder, Colorado campus.

- The non-binding project annex memorandum provides a mutual understanding of the proposed collaboration. Specifically, the memorandum says that the Communication Technology Laboratory at NIST and the Korea Research Institute of Standards and Science intend to participate in:
- Development of advanced precision RF measurement technologies for next-generation superconducting quantum computing.
- Qubit readout and control for scalable low-latency qubit feedback using superconducting circuits.
- Exchange and collaboration on research publications.
- Staff exchanges to conduct joint research at Korea Research Institute of Standards and Science and NIST facilities.

NIST's and KRISS's collaboration will contribute to the global international metrology community in quantum technologies, especially quantum computing and related topics.

3.QuSecure Contributes to White House Quantum Security Roundtable Addressing the Post-Quantum Cybersecurity Threat

by Dan Spalding

https://www.businesswire.com/news/home/20240131064996/en/QuSecure-Contributes-to-White-House-Quantum-Security-Roundtable-Addressing-the-Post-Quantum-Cybersecurity-Threat

QuSecure™, Inc., a leader in post-quantum cryptography (PQC), today announced it was invited to participate and contribute to a key White House Quantum Security Roundtable discussion to consider and help influence the impact from quantum computing on information security. QuSecure offered its unique, customer-driven experience in creating and implementing PQC solutions in both enterprise and government environments to the White House's discussion around the looming post-quantum cybersecurity threat.

"The event was a success and I congratulate the government for collaborating with industry on attempting to address an existential threat," said Aaron Moore, QuSecure EVP of Engineering. "We know that nation states are currently harvesting exabytes of encrypted data that are vulnerable to decryption once a cryptographically relevant quantum computer (CRQC) comes online. The exposure and exploitation of this information and the surprise it creates will be equivalent to what will be in essence the world's greatest recorded ambush."

During the Jan. 26 PQC Migration Roundtable, organized by the Office of the President of the United States and the White House, it was stated that "confidentiality of ephemeral sessions (e.g. TLS) should be the highest priority due to the relative ease of the transition and the threat of store-now-decrypt-later."

Moore also added: "What we need is immediate action. We should incorporate the current PQC algorithms into our systems now by overlaying them on our current cryptographic modules. At worst we have the same level of security that we have today, and at best we become quantum–resilient and begin to future proof our national security."

QuSecure recently won Small Business Innovation Research (SBIR) awards from the U.S. Air Force and the U.S. Army, reinforcing its commitment to work with the federal government. These are examples of QuSecure's leadership and innovation in PQC, a testament to the necessary collaboration between the federal and private sector to quickly and efficiently develop solutions to protect against the emerging threats from AI and quantum computing. This collaboration has been echoed by QuSecure's co-founder and Chief Product Officer Rebecca Krauthamer, who is a member of the World Economic Forum (WEF) Global Futures Council on Quantum. While at the World Economic Forum in Davos earlier this month, Krauthamer said that QuSecure and "the Council help to set the Davos agenda, driving policy and change we collectively need to capitalize on the good while preventing the bad that technology acceleration can bring."

QuSecure's QuProtect software enables organizations to leverage quantum-resilient technology and is currently available to test and deploy, helping to prevent today's cyberattacks, while future-proofing networks and preparing for quantum cyberthreats. It provides quantum-resilient cryptography, anytime, anywhere and on any device including network, cloud, IoT (Internet of Things), edge devices, and satellite communications. Using QuProtect, organizations can implement PQC on the network without removing existing encryption so installation is fast and risk is minimal. QuProtect software uses an end-to-end quantum-security-as-a-service architecture that addresses the digital ecosystem's most vulnerable aspects, uniquely combining zero-trust, next-generation post-quantum cryptography, crypto agility, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed to protect the entire information lifecycle as data is communicated, used and stored.

4.Korea Quantum Computing and IBM Collaborate to Bring IBM watsonx and Quantum Computing to Korea

by Bethany Hill Mccarthy and Chris Nay
https://newsroom.ibm.com/2024-01-29-Korea-Quantum-Computing-and-IBM-Collaborate-to-Bring-IBM-watsonx-and-Quantum-Computing-to-Korea

IBM today announced that Korea Quantum Computing (KQC) has engaged IBM to offer IBM's most advanced AI software and infrastructure, as well as quantum computing services. KQC's ecosystem of users will have access to IBM's full stack solution for AI, including watsonx, an AI and data platform to train, tune and deploy advanced AI models and software for enterprises.

KQC is also expanding its quantum computing collaboration with IBM. Having operated as an IBM Quantum Innovation Center since 2022, KQC will continue to offer access to IBM's global fleet of utility-scale quantum systems over the cloud. Additionally, IBM and KQC plan to deploy an IBM Quantum System Two on-site at KQC in Busan, South Korea by 2028.

"KQC is providing versatile computing infrastructure in Korea through our collaboration with IBM. Our robust hardware computing resources and core software in quantum and AI are poised not only to meet the growing demand for high performance computing, but also to catalyze industry utilization and ecosystem development. We are working to diligently enhance services and infrastructure through this collaboration as well as with our industry-specific partners," said Ji Hoon Kweon, Chairman of KQC.

"We are excited to work with KQC to deploy AI and quantum systems to drive innovation across Korean industries. With this engagement, KQC clients will have the ability to train, fine-tune, and deploy advanced AI models, using IBM watsonx and advanced AI infrastructure. Additionally, by having the opportunity to access IBM quantum systems over the cloud, today — and a next-generation quantum system in the coming years — KQC members will be able to combine the power of AI and quantum to develop new applications to address their industries' toughest problems," said Darío Gil, IBM Senior Vice President and Director of Research.

This collaboration includes an investment in infrastructure to support the development and deployment of generative AI. Plans for the AI-optimized infrastructure includes advanced GPUs and IBM's Artificial Intelligence Unit (AIU), managed with Red Hat OpenShift to provide a cloud-native environment. Together, the GPU system and AIU combination is being engineered to offer members state-of-the-art hardware to power AI research and business opportunities.

To provide a full stack solution, this collaboration will also include access for KQC's clients to Red Hat OpenShift AI for management and runtime needs, and IBM's watsonx platform to empower generative AI and the next wave of computing technology. By leveraging watsonx software for its workflows and solutions, KQC members will have access to generative AI technologies for the enterprise.

In addition to IBM, KQC is also collaborating with other Korean organizations on contributions to the country's quantum computing ecosystem.

"KQC has been actively building quantum research collaborations with leading domestic companies in

the financial, bio-healthcare and pharmaceutical industries. Last year, Dankook University Hospital joined as a co-research member in quantum healthcare. Additionally, as members of our IBM Quantum Innovation Center, Hanlim Pharmaceutical Co., has started joint research for new drug discovery with us. And DNEURO, a Korean financial software start up is developing quantum algorithms in option pricing and portfolio optimization," said Dr. Joon Young Kim, CEO of KQC.

5.Cisco announces new quantum networking collaboration with UK startup

by Greg Noone
https://techmonitor.ai/hardware/quantum/cisco-quantum-networking-nu-quantum

Cisco has announced a new quantum networking collaboration with Nu Quantum, a UK startup. The partnership with Nu Quantum, based in Cambridge, will see Cisco become a prospective end-user for "Lyra," a project that aims to deliver the world's first "Quantum Networking Unit" (QNU.) Funded by a UK government contract valued at £2.3m, the goal is to build a network capable of connecting disparate quantum processing units (QPUs) and massively scale the number of qubits available to researchers and private companies.

"It is increasingly accepted that to reach its potential, quantum networking will be needed to scale quantum computing to a Fault Tolerant era," said Cisco's head of co-innovation, Peter Shearman. "We are delighted to partner with Nu Quantum to accelerate this journey towards a modular, qubit-agnostic and data centre-optimised future."

Quantum networking needed to scale qubit numbers, say experts

Though significant breakthroughs have been made in recent years in raising the number of fault-tolerant qubits in single quantum computers to the double digits, most experts agree that successfully commercialising the field will require networking solutions that combine the raw power of individual machines. One of the loudest advocates of this approach has been IBM, which envisions modular quantum computing circuits powered by its proprietary QPUs.

Nu Quantum's strategy, meanwhile, is platform-agnostic. According to the startup, LYRA will deliver "discrete 19-inch rack-mount [QNU] modules for control-plane and optical interfacing" which are fully upgradable and support various quantum computing modalities. Nu Quantum added that its quantum networking solution also "incorporates a new high-precision timing architecture and digital control bus, allowing the system to easily scale to support a large cluster of quantum-compute nodes."

By using Nu Quantum's QNUs to build quantum computing networks, its founder Carmen Palacios argues, operators will not only be able to harness the requisite number of qubits necessary to solve large and complex problems but also help to move quantum computers out of the laboratory and into data centre-like environments.

Road to the quantum data centre

"A large-scale, fault-tolerant quantum computer will look relatively similar to a high-performance supercomputer today," Palacios told *Tech Monitor*. Alternatively, QNUs could allow for the creation of quantum data centres, wherein "you have four racks of quantum computers and a fifth rack that is the quantum networking unit that is interconnecting all of them."

LYRA is partly funded by a UK government contract won by Nu Quantum in a competition to develop new quantum networking technologies. Founded in 2018 by a team led by Palacios, the firm raised £7m in a pre-series A funding round late last year. It has also previously collaborated with Cisco on the similarly mythological-sounding Project Medusa, where the two collaborated on developing integrated photonic technology to network clusters of trapped ion quantum computers.

Project Lyra follows a series of investments made by Cisco into the field of quantum computing. In March the firm announced its creation of the Cisco Quantum Lab in Santa Monica, California, dedicated to researching quantum security and networking. These fields, said Cisco, would open "near-term commercial markets" for the company as global interest in the technology matures.

6.Cryptographic storage is a secure way to store data using encryption and other security measures.

https://internetstack.com/read/internet-technologies/blockchains/cryptography/cryptographic-storage/

Cryptographic Storage: A Guide

Cryptographic storage is a secure way to store data. It uses encryption to protect data from unauthorized access. In this guide, we'll cover the basics of cryptographic storage, how to use it, best practices, and examples.

Getting Started

Cryptographic storage is a form of data encryption that uses a cryptographic algorithm to protect data from unauthorized access. It is used to protect sensitive data, such as passwords, financial information, and medical records. Cryptographic storage is often used in combination with other security measures, such as firewalls and access control lists.

Cryptographic storage is typically implemented using a cryptographic key. This key is used to encrypt and decrypt data. The key is usually stored in a secure location, such as a hardware security module (HSM) or a secure server. The key is also used to generate a digital signature, which is used to verify the authenticity of the data.

How To

To use cryptographic storage, you'll need to generate a cryptographic key. This key is used to encrypt and decrypt data. You'll also need to store the key in a secure location, such as an HSM or a secure server. Finally, you'll need to generate a digital signature to verify the authenticity of the data.

Once you have the key and the digital signature, you can start encrypting and decrypting data. To encrypt data, you'll need to use a cryptographic algorithm, such as AES or RSA. To decrypt data, you'll need to use the same cryptographic algorithm and the same key.

Best Practices

- Always use a strong cryptographic algorithm, such as AES or RSA.
- Store the cryptographic key in a secure location, such as an HSM or a secure server.
- Generate a digital signature to verify the authenticity of the data.
- Ensure that the cryptographic key is kept secure and is not shared with anyone.
- Ensure that the cryptographic algorithm is regularly updated to keep up with advances in technology.
- Ensure that the cryptographic key is regularly changed to prevent unauthorized access.

Examples

Here are some examples of cryptographic storage in action:

- A bank uses cryptographic storage to protect customer financial information.
- A healthcare provider uses cryptographic storage to protect patient medical records.
- A government agency uses cryptographic storage to protect classified information.
- A software company uses cryptographic storage to protect source code.

7.Is Q-Day — The Day Quantum Computing Hacks Everything — Approaching?

by Ray Fernandez
https://www.techopedia.com/q-day-is-coming-how-experts-secure-quantum-computing

Quantum technology is the always just-out-of-reach next chapter of technology. But every week, it gets closer.

With never-seen-before computation skills and mathematical potential, scientists predict quantum computing will finally crack “impossible” problems in astrobiology, physics, and mathematics, let alone impact our daily lives.

Pharmaceutical and medical organizations hope to use quantum computing to discover new drugs, cure ‘uncurable’ diseases, and design new treatments while engineers seek to develop materials and concepts. Meanwhile, machine learning developers look to achieve artificial superintelligence.

Additionally, industries such as the global financial industry — where fast math makes the difference between gains and losses — anxiously await for quantum computing to become the norm.

However, despite the dazzling future that quantum technology promises, it also casts a sinister shadow — Q-Day.

Q-Day 101: The Beginning of the End?

Numerous experts and organizations have already given estimates — some conservative and others for the next five to ten years — for the day quantum computing will reach performance levels that allow it to break the encryption algorithms used in our digital world.

From phone calls to emails, passwords, financial account credentials, administrative access, and even top-secret confidential documents and data… if and when Q-Day hits us, there is nothing that a quantum computer in the wrong hands would not be able to decrypt.

Q-Day may sound like something out of a science fiction movie, but it is something analysts say is a likely reality. Governments, organizations, academia, regulators, security experts, and cryptographers worldwide are already working in quantum resilient encryption and quantum security.

They believe it's not a matter of when Q-Day arrives but whether the world will be ready when it knocks on the door.

NSA, CISA, and Intelligence Agencies Send A Flare Message

In 2022, the NSA called on organizations of all sizes to move to quantum-safe encryption by 2035. Adding to the call for security, in 2023, CISA, NSA, and NIST published a new resource with guidelines for migrating to post-quantum cryptography.

"It is imperative for all organizations, especially critical infrastructure, to begin preparing now for migration to post-quantum cryptography," CISA director Jen Easterly said back then and recognized transition difficulties.

"The transition to a secured quantum computing era is a long-term intensive community effort that will require extensive collaboration between government and industry. The key is to be on this journey today and not wait until the last minute."

Tim Hollebeek, industry technology strategist at DigiCert, told Techopedia: "Systems and data that need to be secure for a long time into the future are the most important.

"This includes things like firmware signing, signatures that need to be trusted for years, and stored data and network transmissions that need to be secret for a decade or more."

Sanzeri said that the old-fashioned public-key encryption algorithms used for nearly half a century to protect government secrets and intellectual property are no longer practical.

Sanzeri added that the White House executive order "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" outlines several near-term security directives, making room for quantum-resilient cryptography and post-quantum communications.

"If the United States wants to protect itself from quantum computing attacks, it must switch to post-quantum cryptography protocols. This is a pressing matter of national security, and the government has already begun to act on this issue."

Howling Wolf: Has the Quantum Threat Been Oversold?

Quantum computers are not new, and the hype about the tech and the concerns for the potential dam-

age it might cause have been around for some time. These warnings of dangerous events have yet to materialize — and the question follows: "Is Q-Day a myth or a future reality?"

Or, more specifically: "Should leaders take Q-day seriously, and why now?"

Skip Sanzeri, co-founder, CFO, and COO of QuSecure, a leading post-quantum security company that aims to protect enterprises and governments from the threat of quantum computers, says:

"This problem (Q-Day) necessitates immediate attention on both the national and international scales. Although quantum technologies offer many potential benefits to humankind, they could have a much more significant negative impact if this risk comes to fruition."

Sanzeri added that if current encryption methods become obsolete, enterprises, digital infrastructures, and economies — that rely on this type of security — will be significantly impacted.

"Data stolen now will be decrypted once Q-Day is here. Because we have yet to determine when Q-Day will happen, it's tough to decide when the best time is to act. This usually leads to de-prioritization in favor of more pressing issues; however, this may be just kicking the quantum can down the road."

At Clarksdale Crossroads: Google, Microsoft, IBM, and Amazon's Cloud Quantum Computing

Global leading cloud vendors like IBM, Microsoft, Google, Amazon, and others already offer their customers access to quantum cloud computing resources. Cloud quantum computing is expected to be the main channel for the world to access these incredibly hard-to-engineer and super-expensive machines.

Have these cloud quantum machines reached performance levels linked to Q-Day, and can they break global encryptions?

Hollebeek gave insight into these early quantum computer cloud systems offering services to users.

"Not all quantum computers can threaten traditional encryption. A quantum computer powerful enough to threaten RSA and ECC is known as a cryptographically relevant quantum computer (CRQC), and those don't exist yet."

Going into technical details, Hollebeek explained that today's quantum computers only have hundreds to one thousand noisy qubits being used to create a handful of stable, error-corrected ones.

"A CRQC needs to have thousands of stable qubits, which probably requires millions of noisy ones to implement. So while the capabilities of quantum computers are rapidly advancing, they aren't quite to the point where they threaten classical encryption, but probably will get there in the next 5-10 years or possibly sooner."

Patrick Scully, director at Ciena, is currently leading the company's work to develop optical encryption for the quantum age told Tecopedia that leaders should be aware of "harvest now, decrypt later" — a new cybercriminal technique in which bad actors are stealing encrypted data and storing it to decrypt it in the future.

"Organizations with data that retains its value over time should be considering mitigation measures quite seriously."

Scully is working on Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD), But PQC algorithms are currently undergoing standardization proof and do not guarantee full security.

However, the route they are working towards follows the lines of:

"QKD systems are considered to provide unconditional security, as the security of the key is not based on the computational complexity of mathematical problems, but rather on the laws of physics."

A Quantum Time Travel Security Game: Build Now To Secure 2030

"Many experts in the industry, including Forrester, think the chances of Q-Day happening before 2030 is over 50%," Dr. Kristin Gilkes, global innovation quantum leader at EY, told Techopedia.

"Even if the odds were the same as a coin toss, I would not advise clients to leave their most prized secrets to mere chance."

From Forrester's end, last year, they stated:

"Forrester estimates that within five to 15 years quantum computing will render existing mainstay asymmetrical cryptographic algorithms wholly or at least partially unusable for protecting sensitive information."

Dr. Gilkes explained that quantum security is about how fast quantum computing advances and how long it will take businesses to "completely overhaul their security infrastructure".

Taming The Wild West of Quantum Computing

Cloud brands like Google, Microsoft, IBM, Amazon, and others are the only companies with the budget, resources, and skills needed to develop, build, and operate advanced quantum computers. This raises numerous legal, compliance, and ethical questions.

"Most cloud providers are not yet offering quantum resilient encryption," Sanzeri said. "However, we expect this to change over time. Large infrastructure providers must move quickly to begin installing post-quantum cybersecurity to protect their customers.

"Even if cloud providers deploy quantum resilient encryption, the enterprise still needs to protect their internal communications networks and their customer and partner networks."

Businesses and governments are already taking steps to protect themselves against the threat of quantum computing. "One way they are doing this is by implementing post-quantum cryptography," Sanzeri said.

"The great news is that you don't need a quantum computer to fight against a quantum computer; we can use classical math and software."

Criminals in the Underground "Harvest Now, Decrypt Later"

We asked cybersecurity sources basic questions on the criminal trend "harvest now, decrypt later" and wanted to know what cyber gangs or nation-state-supported cybercriminal groups were active in quantum computing attacks.

DigiCert's global study: "Preparing for a Safe Post-Quantum Computer Future," reveals that more than half (61%) of IT leaders are concerned that their organization will not be prepared for quantum computing cyberattacks.

Even more organizations, 74% of them, say they are worried about "harvest now, decrypt later" attacks. Despite these evident pain points, the companies seem to be at a loss on what to do next.

"Many organizations are in the dark about the characteristics and locations of their cryptographic keys."

According to the study, IT leaders believe time is against them, and 41% say the Q-Day countdown is set for just five years.

Budget, skills, lack of leadership, and awareness of the real risks of quantum computing security implications are the main challenges they mention in the study.

Pre-Emptive Action

Dr. Gilkes said that replacing the traditional RSA encryption with new cryptographic algorithms based on quantum computing is broadly considered the far more secure option in the threat of a quantum-based cyberattack.

The bad news? This involves a large (and expensive) replacement of the existing security infrastructure.

For those looking for technical guidelines, they can also check the upcoming National Institute of Science and Technology (NIST) Post-Quantum Cryptography standards, expected sometime in 2024.

Dr. Gilkes added that Quantum Key Distribution — leveraging unique properties of quantum mechanical systems to generate and distribute cryptographic keying material — can be done over the cloud. This is an easier option for those who want to implement quantum security on top of existing IT infrastructure. However, these systems have risks as they can open doors to attack vectors.

For those who think their organization is not a target, Sanzeri said that quantum security affects all types of organizations, from federal governments to critical infrastructure facilities, satellites, financial services, enterprises, and more.

The Bottom Line

We don't think this one is an overblown threat. Q-Day looks to be a tentative entry in the calendar, we just don't know when the clock will strike midnight. Acknowledging that potential is the first step to securing the future.

We exercise caution in giving the final word to companies that offer to be part of the solution.

Still, on this occasion, we'll let Sanzeri paint his predicted scenario and let you decide how much weight you want to assign to the warning:

"Make no mistake, if public-key cryptography starts breaking, this will prove to be an existential threat to our nation, allies, and the free world."

8.What is the quantum threat and what has simple maths got to do with protecting global security?

by Pascale Davies

https://www.euronews.com/next/2024/01/26/what-is-the-quantum-threat-and-what-has-simple-maths-got-to-do-with-protecting-global-secu

There may come a day known as Q-Day, which will shatter global security as we know it.

It could be in a few years from now, or in 10 years or more. But scientists, mathematicians, and governments are not waiting idly by for the quantum threat to happen.

Q-Day is when a **quantum computer** so powerful is built, it could break the public encryption systems that protect our online conversations, bank accounts, and most vital infrastructure, wreaking havoc on governments and businesses.

How this digital doomsday would happen comes down to simple maths.

How it started

Since the beginning of the Internet, cryptography has protected our online data and conversations by hiding or coding information that only the person receiving the message can read on traditional computers.

In the 1970s, mathematicians built encryption methods that consisted of numbers hundreds of digits long. The difficulty of mathematical problems was such that it could take at hundreds of years to solve if using the right parameter size and numbers.

To break the encryption, the numbers need to be split into their prime factors, but this could take hundreds if not thousands of years with traditional computers.

The threat of codes being cracked was therefore not a big worry.

That was until 1994 when the American mathematician Peter Shor showed how it could be done with an algorithm using a then hypothetical quantum computer that could split large numbers into their factors much quicker than a traditional computer.

The rise of quantum

The quantum threat was still not a significant concern back then but it started to become an issue four years later when the first quantum computer was built.

Though that quantum computer - and those currently being built - are still not powerful enough to use Shor's algorithm to decrypt the numbers, in 2015, intelligence agencies determined that the advancement in quantum computing is happening at such a speed that it poses a threat to cyber security.

At the moment, qubits, the processing units of quantum computers, are not stable for long enough to decrypt large amounts of data.

But tech companies such as IBM and Google have slowly but steadily started making progress in building machines strong enough to deliver the benefits of quantum, which include pharmaceutical research, subatomic physics, and logistics.

"It's a matter of time and it's a matter of how long does it take until we have a large quantum computer to go," Dr Jan Goetz, CEO and co-founder of IQM Quantum Computers, a start-up that builds quantum computers, told Euronews Next.

If it takes 30 years to build a strong enough computer, there would be less reason to panic as most of the encrypted data might no longer be relevant.

But “if someone comes up with a very clever idea and can already, do the code-breaking in 3 to 5 years, the whole situation also looks different,” Goetz said.

Who should be worried?

Individuals should not be concerned by Q-Day as there are probably few people who have data that is very sensitive and will still be relevant in years to come.

Goetz said once the new technology comes, encryption codes will be updated on all computers and phones and “you should not be too concerned about this because the industry will take care of this”.

But governments, organisations, and businesses should be concerned by the quantum threat.

There is a concept called “store now, decrypt later”. It means someone could be storing the data and waiting for a quantum computer strong enough to come along and decrypt it.

“Governments in particular are harvesting data from the Internet,” said Dr Ali El Kaafarani, founder and CEO of quantum-safe cryptography company PQShield.

“They are storing data that they can't access or read at the moment, but they can keep them there until the cryptography layer becomes weaker until they know of a way to attack it and then they break it and they read those communications,” he told Euronews Next.

A post-quantum cryptography world

Governments are not standing by for that to happen and the cryptographic community are building encryption methods that can withstand the quantum threat, known as post-quantum cryptography (PQC).

This year, sometime between May and June, the final standardisation of PQC will be released by the US National Institute of Standards and Technology.

This will be a game-changer as it will be on the market for all industries.

The US legislation has mandated that the timeline to change to PQC will be from 2025 until 2033, by which time the cyber secure supply chain will have to have transitioned to using PQC by default.

In 2025, web browsers and software updates will have to become post-quantum secure by default if they are sold to the US, said El Kaafarani.

This is why some companies, such as Google Chrome and Cloudflare, have already started using PQC.

The US’s PQC standards are international standards, but every country has their own guidelines governments do collaborate.

The US, UK, French government, German, and Dutch governments, among others, have all weighed in and produced whitepapers and guidelines for the industry to push them to start the transition phase to post-quantum cryptography as they understand that it is a process that will take time.

“Governments take care of standardising the algorithms so that we all speak the same language,” said El Kaafarani, but it is the cryptographic community that comes up with the new encryption methods that

are not vulnerable against quantum computers.

Most of the cryptographic standards are developed in Europe by European cryptographers, he added, whose UK-based company had four encryption methods selected to be in the US's PQC standards.

Once developed, the encryption methods are ruthlessly scrutinised by the wider cryptographic community, governments, and everyone else who is interested in cracking the encryption methods.

"Some get broken along the way. And that's the whole point of the process, is to root out the weak ones and keep them the strong ones," said El Kaafarani.

But there is no perfect encryption method or security method that can ensure that everything will stay secure forever.

"Therefore cryptography is naturally an evolving field and that's why we need to keep ahead and keep an eye on how things are evolving," he said.

9.DORA and your quantum-safe cryptography migration

by Dinesh Nagarajan and Joachim Schäfer
https://securityintelligence.com/posts/dora-quantum-safe-cryptography-migration/

Quantum computing is a new paradigm with the potential to tackle problems that classical computers cannot solve today. Unfortunately, this also introduces threats to the digital economy and particularly the financial sector.

The Digital Operational Resilience Act (DORA) is a regulatory framework that introduces uniform requirements across the European Union (EU) to achieve a "high level of operational resilience" in the financial services sector. Entities covered by DORA — such as credit institutions, payment institutions, insurance undertakings, information and communication technology (ICT) service providers, etc. — are expected to comply by January 17, 2025.

New requirements for financial entities in the EU

DORA lays out a set of requirements across ICT risk management, incident reporting, operational resilience testing, cyber threat and vulnerability information sharing, and third-party risk management. As part of those requirements and in the context of data protection and cryptography, it lays out in Article 9 ("Protection and prevention") that financial entities "shall use ICT solutions and processes" that "(a) ensure the security of the means of transfer of data" or "(c) prevent […] the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data."

Further elements to consider in the context of Article 9 are referred to in Article 15 and laid out in the related (draft) regulatory technical standards, which the ESA published on January 17, 2024. Particularly, JC 2023 86 provides detailed requirements on cryptographic guidance. In addition, in its preambles, the following is stated:

"Given the rapid technological developments in the field of cryptographic techniques, financial entities […] should remain abreast of relevant developments in cryptanalysis and consider leading practices and

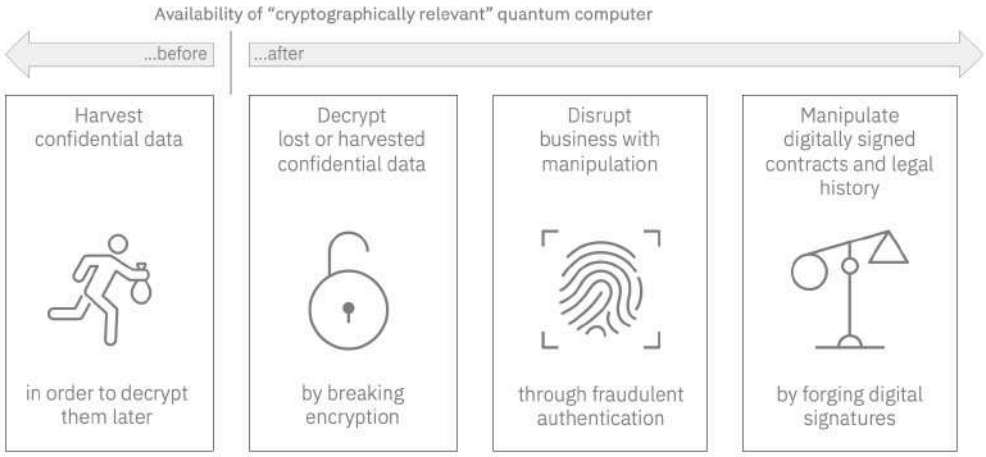
standards and should hence follow a flexible approach based on mitigation and monitoring to deal with the dynamic landscape of cryptographic threats, including those from quantum advancements."

Below, we will further elaborate on the referred 'cryptographic threats' and the implications they could have on financial institutions in the context of quantum computing.

Quantum threats and quantum-safe cryptography

While current quantum computers still struggle with noise and are not yet "fault-tolerant," impressive milestones have been reached already proving their utility. Given the number of investments being made in both the private sector and academia, it is expected that this technology will scale and drastically improve over time. As it does, the potential threat to the digital economy will grow.

In 1994, the physicist Peter Shor introduced an algorithm that, when run on a large-scale quantum computer, could break public key-cryptography algorithms such as Rivest-Shamir-Adleman (RSA), Diffie-Hellman and Elliptic Curve Cryptography (ECC). The financial sector relies on these algorithms to ensure the confidentiality and integrity of bank transactions, the authenticity of its customers, the validity of digitally signed documents and the confidentiality of customer financial data. If the supporting cryptography can no longer be trusted, the entire financial sector is at risk.



Quantum threats posed to cryptography

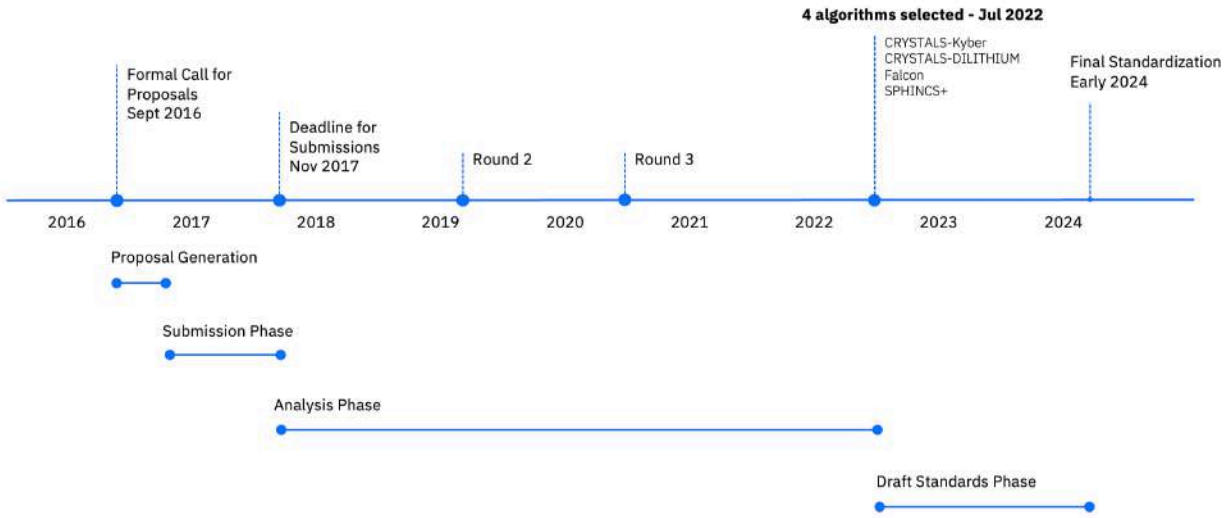
To break today's cryptography, a so-called Cryptographically Relevant Quantum Computer (CRQC) would need to be realized (some experts estimate it could happen in the early 2030s). However, while the impact is in the future, we are at risk already. One can imagine an attacker harvesting encrypted confidential data today to decrypt it later.

Fast-tracking quantum-resistant cryptography

NIST standardization timeline for quantum-safe (aka 'post-quantum') cryptography

Fortunately, new "quantum-safe" cryptography is being standardized, with the most noteworthy effort being run by the National Institute of Standards and Technology (NIST). In 2016, NIST launched a competition with more than 80 submissions to standardize a new form of cryptography that will run on ordinary systems (e.g., laptops, cloud, etc.) but will be resistant to a quantum attacker because it relies on mathematical problems that are hard to solve by a quantum (and classical) computer.

The first four algorithms for standardization were selected by NIST in July 2022 (out of which three were co-contributed by IBM). While the standards are planned to be released in 2024, additional alternate



candidates are still being considered.

A quantum-safe cryptography standard is in sight. Unfortunately, due to the complexity of the financial sector in particular, a lengthy journey lies ahead. NIST assumes that "five to 15 or more years will elapse […] before a full implementation of those standards is completed." If we overlay this with the development timelines of a CRQC, one realizes that entities have to start this journey today.

Why quantum has an impact on DORA

Quantum threats, when they materialize, have the potential to drastically impact the operational resilience of financial entities and could disrupt the economy globally. Fortunately, new quantum-safe cryptography algorithms are available (with standards very soon to be published), which will be needed to mitigate those threats.

If we relate this to the requirements of DORA, we can draw several direct links. To satisfy Article 9, financial entities will need to adopt quantum-safe means of data transfer, as well as quantum-safe mechanisms to "prevent […] the impairment of the authenticity and integrity, the breaches of confidentiality and loss of data."

This implies the need to adopt upcoming, quantum-safe data-in-transit protocols such as quantum-safe transport layer security (TLS) or quantum-safe virtual private networks (VPNs), as well as quantum-safe mechanisms for signing (legally binding) documents or bank transactions. As a result, financial entities will need to implement supporting infrastructure such as quantum-safe public key infrastructure (PKI) and key management systems.

Additionally, implementations today are often in the hands of third-party suppliers. To add to the complexity, in many cases, existing programs, such as a "move to cloud" or "zero trust" implementation, will be impacting several of the above-mentioned elements.

Quantum threats can have serious consequences

In a worst-case scenario, if financial services organizations do not remediate quantum threats in their digital ecosystem, this can impact the resilience of their business by:

- Being unable to verify authorized users on their network leads to confusion and a complete lack of

trust in their digital ecosystem.

- Being unable to fulfill their data privacy regulations due to a lack of trust in the mechanisms (e.g., encryption) used to protect such data.
- Increased risk of exposure to external threats from the presence of vulnerable cryptography protocols and algorithms on business-to-business and supply chain networks.
- Disruption of day-to-day business from downtime required to remediate digital services and applications.

Given current draft requirements as per JC 2023 86, one can anticipate that soon after quantum-safe cryptography is standardized, it will be considered an account-leading practice. Hence, regardless of when quantum threats might materialize, regulatory requirements, such as DORA, will soon implicitly mandate the adoption of quantum-safe cryptography in the financial industry.

At the same time, organizations should seize the opportunity to improve their overall cryptographic agility by modernizing the way cryptography is implemented today and making future changes much more timely and cost-efficient.

Implement your quantum-safe migration

It is clear that implementing quantum-safe cryptography will not be an easy endeavour. Such a migration program will require agility and also offers the possibility to exploit an early mover advantage. It will require a multi-pronged approach, including top-down business priorities as well as bottom-up technical capabilities.

We recommend the following steps that organizations impacted by DORA should take at a minimum:

Assess and review your enterprise cryptographic posture and identify elements (applications, networks, strategic projects, etc.) potentially impacted by quantum threats.

Develop a plan based on business priorities and take into account synergies with existing transformation programs, laying out an approach to remediation for the impacted digital services and corresponding systems.

Improve your cryptographic posture by introducing cryptographic discovery and inventory capabilities. Introduce cryptographic observability to validate cryptographic compliance on an ongoing basis, including leveraging "cryptography bills of material." Such elements will increase the cryptographic agility of your organization.

Ensure current change processes and strategic projects take into consideration the impact of cryptography and provisions are made to implement remediation on the least disruptive basis.

Sponsor a program to continue the steps above continually.

Above all, do not wait to begin tackling these steps. We strongly recommend that organizations define a quantum-safe migration program today.

10.A Detailed Journey with Olivia Lanes Exploring the IBM Quantum Lab, Reveals the Intricacies of Quantum Computing

by James Dargan
https://thequantuminsider.com/2024/01/25/a-detailed-journey-with-olivia-lanes-exploring-the-ibm-quantum-lab-reveals-the-intricacies-of-quantum-computing/

In a fascinating tour of an IBM Quantum lab and data center, Dr. Olivia Lanes, Global Lead and Manager for IBM Quantum Learning and Education, provided an in-depth look into the world of quantum computing. The tour, which explored the complex workings of quantum computers and their environment, offered rare insights into this cutting-edge technology.

Lanes, an experienced scientist and educator in the field, commenced the tour by highlighting IBM Quantum's achievement.

"IBM Quantum has the largest number of quantum processors available through the cloud," she said, underscoring IBM's leading role in the quantum computing space.

One of the tour's focal points was the dilution refrigerator, essential for maintaining the extremely low temperatures necessary for quantum computing. Lanes described this sophisticated equipment as a "Russian nesting doll," a layered structure designed to progressively cool its contents.

"The outer can here is obviously at room temperature…the inner can which hosts the IBM Quantum processor and lives here at the very bottom is at an insanely cold temperature of about 15 millikelvin," said Lanes.

Lanes explained the process of communicating with the quantum processors, a complex task due to their cryogenic environment.

"We basically have cables that run to the bottom of the fridge here and then all the way back up to the top of the fridge into these room temperature amplifiers," she said. This intricate system allows the quantum signals to be amplified and processed by standard computing devices.

The tour also revealed the substantial infrastructure supporting these quantum systems. Lanes pointed out various components, including pumps, compressors and liquid nitrogen tanks, all crucial for maintaining the delicate conditions needed for quantum computing.

"We need to make sure that this drawer of liquid nitrogen is full at all times," she said, underlining the continuous need for these resources.

Lanes also showcased the control systems that manage the cryogenic environment. She illustrated the ease of operation, saying: "The laptop here is also an interface for all of the cryogenic equipment in the dilution refrigerator as well. You can log on and basically press one button that says full cool down or one button that says full warmup."

The tour provided a unique glimpse into the world of quantum computing, demystifying the complex

machinery and processes behind this revolutionary technology. Lanes' expertise and the detailed exploration of the IBM Quantum lab illuminated this often misunderstood cutting-edge science and sophisticated engineering that powers quantum computers. This field, still in its nascent stages, holds immense potential for future technological advancements, and IBM's work exemplifies the progress being made in making quantum computing a reality.

11.Chinese scientists realize crosstalk-avoided quantum network node

by CGTN
https://news.cgtn.com/news/2024-01-24/Chinese-scientists-realize-crosstalk-avoided-quantum-network-node-1qDdI9vIMlW/p.html

Chinese scientists have made an advance in quantum networking by achieving, for the first time, a crosstalk-avoided quantum network node using dual-type qubits of the same ion species.

Qubit, or quantum bit, is the basic unit of information in quantum computing. One of the most promising physical systems for quantum networks at present is the ion trap. In such a network, the ion-photon entanglement is the basic unit, but it would affect memory qubits carrying quantum information and cause an information loss, which is known as crosstalk.

To avoid crosstalk, two ion species are commonly used to, respectively, entangle with photons and store quantum information. However, this dual-species scheme has limitations such as high device cost for different ions and high requirements for operations.

A research team from Tsinghua University proposed a quantum network node where only a single ion species was needed, but with two types of qubits. They published the findings recently in the journal Nature Communications.

In the findings, the same kind of ions in the quantum network node were encoded in two different hyperfine structure levels, one for entanglement with photons and the other for information storage, said Huang Yuanyuan, a team member at Tsinghua University.

Huang noted the ion-photon entanglement was generated in a typical timescale of hundreds of milliseconds, and its crosstalk on the memory qubit was verified to be negligible at the experimental precision.

The new scheme, on the premise of ensuring the effect of ion-photon entanglement and information storage, has greatly simplified the hardware system of quantum networking and taken a significant step towards its future development, said Duan Luming, the team leader at Tsinghua University.

12.Cryptographers Just Got Closer to Enabling Fully Private Internet Searches

by Madison Goldberg

https://www.wired.com/story/cryptographers-fully-private-internet-searches-cybersecurity-databases-privacy/

We all know to be careful about the details we share online, but the information we seek can also be revealing. Search for driving directions, and our location becomes far easier to guess. Check for a password in a trove of compromised data, and we risk leaking it ourselves.These situations fuel a key question in cryptography: How can you pull information from a public database without revealing anything about what you've accessed? It's the equivalent of checking out a book from the library without the librarian knowing which one.

Concocting a strategy that solves this problem—known as private information retrieval—is "a very useful building block in a number of privacy-preserving applications," said David Wu, a cryptographer at the University of Texas, Austin. Since the 1990s, researchers have chipped away at the question, improving strategies for privately accessing databases. One major goal, still impossible with large databases, is the equivalent of a private Google search, where you can sift through a heap of data anonymously without doing any heavy computational lifting.

Now, three researchers have crafted a long-sought version of private information retrieval and extended it to build a more general privacy strategy. The work, which received a Best Paper Award in June 2023 at the annual Symposium on Theory of Computing, topples a major theoretical barrier on the way to a truly private search.

"[This is] something in cryptography that I guess we all wanted but didn't quite believe that it exists," said Vinod Vaikuntanathan, a cryptographer at the Massachusetts Institute of Technology who was not involved in the paper. "It is a landmark result."

The problem of private database access took shape in the 1990s. At first, researchers assumed that the only solution was to scan the entire database during every search, which would be like having a librarian scour every shelf before returning with your book. After all, if the search skipped any section, the librarian would know that your book is not in that part of the library.

That approach works well enough at smaller scales, but as the database grows, the time required to scan it grows at least proportionally. As you read from bigger databases—and the internet is a pretty big one—the process becomes prohibitively inefficient.

In the early 2000s, researchers started to suspect they could dodge the full-scan barrier by "preprocessing" the database. Roughly, this would mean encoding the whole database as a special structure, so the server could answer a query by reading just a small portion of that structure. Careful enough preprocessing could, in theory, mean that a single server hosting information only goes through the process once, by itself, allowing all future users to grab information privately without any more effort.

For Daniel Wichs, a cryptographer at Northeastern University and a coauthor of the new paper, that seemed too good to be true. Around 2011, he started trying to prove that this kind of scheme was impossible. "I was convinced that there's no way that this could be done," he said.

But in 2017, two groups of researchers published results that changed his mind. They built the first programs that could do this kind of private information retrieval, but they weren't able to show that the programs were secure. (Cryptographers demonstrate a system's security by showing that breaking it is as difficult as solving some hard problem. The researchers weren't able to compare it to a canonical hard problem.)

So even with his hope renewed, Wichs assumed that any version of these programs that was secure was still a long way off. Instead, he and his coauthors—Wei-Kai Lin, now at the University of Virginia,

and Ethan Mook, also at Northeastern—worked on problems they thought would be easier, which involved cases where multiple servers host the database.

In the methods they studied, the information in the database can be transformed into a mathematical expression, which the servers can evaluate to extract the information. The authors figured it might be possible to make that evaluation process more efficient. They toyed with an idea from 2011, when other researchers had found a way to quickly evaluate such an expression by preprocessing it, creating special, compact tables of values that allow you to skip the normal evaluation steps.

That method didn't produce any improvements, and the group came close to giving up—until they wondered whether this tool might actually work in the coveted single-server case. Choose a polynomial carefully enough, they saw, and a single server could preprocess it based on the 2011 result—yielding the secure, efficient lookup scheme Wichs had pondered for years. Suddenly, they'd solved the harder problem after all.

At first, the authors didn't believe it. "Let's figure out what's wrong with this," Wichs remembered thinking. "We kept trying to figure out where it breaks down."

But the solution held: They had really discovered a secure way to preprocess a single-server database so anyone could pull information in secret. "It's really beyond everything we had hoped for," said Yuval Ishai, a cryptographer at the Technion in Israel who was not involved in this work. It's a result "we were not even brave enough to ask for," he said.

After building their secret lookup scheme, the authors turned to the real-world goal of a private internet search, which is more complicated than pulling bits of information from a database, Wichs said. The private lookup scheme on its own does allow for a version of private Google-like searching, but it's extremely labor-intensive: You run Google's algorithm yourself and secretly pull data from the internet when necessary. Wichs said a true search, where you send a request and sit back while the server collects the results, is really a target for a broader approach known as homomorphic encryption, which disguises data so that someone else can manipulate it without ever knowing anything about it.

Typical homomorphic encryption strategies would hit the same snag as private information retrieval, plodding through all the internet's contents for every search. But using their private lookup method as scaffolding, the authors constructed a new scheme which runs computations that are more like the programs we use every day, pulling information covertly without sweeping the whole internet. That would provide an efficiency boost for internet searches and any programs that need quick access to data.

While homomorphic encryption is a useful extension of the private lookup scheme, Ishai said, he sees private information retrieval as the more fundamental problem. The authors' solution is the "magical building block," and their homomorphic encryption strategy is a natural follow-up.

For now, neither scheme is practically useful: Preprocessing currently helps at the extremes, when the database size balloons toward infinity. But actually deploying it means those savings can't materialize, and the process would eat up too much time and storage space.

Luckily, Vaikuntanathan said, cryptographers have a long history of optimizing results that were initially impractical. If future work can streamline the approach, he believes private lookups from giant databases may be within reach. "We all thought we were kind of stuck there," he said. "What Daniel's result gives is hope."

13.Preparing for Post-Quantum Cryptography: Trust is the Key

by Lawrence Liu
https://embeddedcomputing.com/technology/security/preparing-for-post-quantum-cryptography-trust-is-the-key

The era of quantum computing is on its way as governments and private sectors have been taking steps to standardize quantum cryptography. With the advent of the new era, we are faced with new opportunities and challenges. This article will outline the potential impact of quantum computing and discuss strategies for preparing ourselves amid these anticipated changes.

In 1980, Paul Benioff first introduced Quantum Computing (QC) by describing the quantum model of computing. In classical computing, data is processed using binary bits, which can be either 0 or 1, whereas quantum computing uses quantum particles called “qubits.” Qubits can be in multiple states beyond 0 or 1, making them much faster and more powerful to perform calculations than a normal bit. To be more specific, with a quantum computer, we can finish a series of operations that would take a classical computer thousands of years in just hundreds of seconds. In fact, IBM just launched the first quantum computer with more than 1,000 qubits in 2023.

Nevertheless, the speed boost of quantum computing can have double-edged consequences. Modern cryptographers have been concerned about the potential impacts on the security of public-key crypto algorithms. Those regarded as unbreakable are now at risk, as a cryptographically relevant quantum computer (CRQC) can do short work of decryption. For instance, the most popular public-key cryptosystem, Rivest-Shamir-Adleman (RSA), was previously considered very challenging with its complex inverse computation. However, in Shor’s algorithm where quantum speedup is particularly evident, the once reliable computation time becomes CRQC-vulnerable. As such, the US National Institute of Standards and Technology (NIST) has been promoting the standardization of post-quantum cryptography (PQC). In addition, the National Security Memorandum (NSM-10) was issued in 2022 in response to the threat brought by cryptographically relevant quantum computers (CRQC).

In fact, when it comes to quantum computing, there are still many issues that researchers cannot agree on. In the current “noisy intermediate scale quantum” (NISQ) era, it is still unclear what the ideal architecture of a quantum computer is, when we can expect the first CRQC, and how many qubits we will need for a quantum computer. Take the “minimum number of qubits would qualify a quantum computer” as an example. Google estimated that it may be 20 million qubits. But with a different quantum algorithm, Chinese researchers in 2022 proposed their own integer factoring algorithm, claiming that only 372 qubits are needed to break a 2048-bit RSA key.

Despite the various quantum computing issues, researchers have a consensus on the necessity and urgency of the PQC transition. Based on the guidelines proposed by both public and private sectors, we have concluded the following key points for a smooth PQC transition:

1. Create an inventory of critical data and existing cryptographic systems at risk, particularly public-key algorithms such as digital signatures/key exchange.

2. Consider how long the at-risk data is to be protected, how valuable the data/asset is to the organization, and how much exposure or shielding the system has from external systems.

3. Check in with/engage the standards organizations regarding the latest PQC updates, such as the NIST.

4. Create a plan/timeline for transitioning to PQC.

5. Stay crypto-agile and implement a phased migration to PQC with hybrid mechanisms that are compatible with the new standards as well as the classical ones before a complete switchover.

6. Alert and educate staff members of PQC transition and schedule training sessions.

The above suggestions are, in fact, not dependent on the PQC standards, and the preparations can start now. It is important to keep in mind that overall system security remains the top priority in both classical computing and the PQC era. The scope of the transition will not really affect all the classical cryptographic algorithms we are familiar with. That is, the current NIST-recommended AES-256 cipher and SHA-384 hash algorithms are still acceptable (yet not satisfying) in the post-quantum world.

The full transition to PQC may span many years, giving us more time to examine PQC readiness and stay crypto-agile. According to the National Security Memorandum (NSM-10), the winners of the final round of NIST's PQC Standardization are expected to be announced in 2024, so organizations are suggested to start the timer then. Table 1 compares those algorithms that have already been selected for NIST standards with their classical counterparts in terms of public key and ciphertext/signature size (in bytes). More importantly, any systems built today should maintain the ability to stay flexible enough to account for possible future modifications, understanding that what may appear quantum-safe today may not be so soon.

Name	(Size in bytes)			Post-quantum?	Related Standard	Comment
	public key	ciphertext	signature			
CRYSTALS-Kyber-512	800	768	n/a	Y	FIPS 203	Lattice-based public key encapsulation mechanism
RSA-2048	256	256	256	N	FIPS 186-5 IETF RFC 8017	Rivest-Shamir-Adleman encryption/signature
CRYSTALS-Dilithium	1312	n/a	2420	Y	FIPS 204	Lattice-based signature
Falcon-512	897	n/a	666	Y	Coming soon	Lattice-based signature
SPHINCS+ 128s	32	n/a	7856	Y	FIPS 205	Stateless hash-based signature
SPHINCS+ 128f	32	n/a	17088	Y	FIPS 205	Stateless hash-based signature
Ed25519	32	n/a	64	N	FIPS 186-5 IETF RFC 8032	Elliptic curve-based signature
LMS	56	n/a	2508	Y	NIST SP800-208 IETF RFC 8554	Stateful hash-based signature
XMSS	68	n/a	2500	Y	NIST SP800-208 IETF RFC 8391	Stateful hash-based signature

Table1: Candidates of NIST's PQC Standardization

Security concerns and levels will continue to evolve as quantum computing advances. This makes a more robust safety storage system, such as NeoPUF, necessary. When all is said and done, security is all about trust. Without the foundation of trust, the classical RSA public-key algorithm or a lattice-based PQC algorithm becomes ineffective. Since important system keys should be highly random and unable to be guessed, the secure methods for creating trust in a system will become increasingly important in the post-quantum world. An even stronger base of trust, a hardware root of trust (HRoT), must be implemented in the hardware, as the software root of trust alone is no longer considered sufficient. The most robust form of such internal provisioning is PUF-based. Having delivered trust on multiple foundry platforms, eMemory and its subsidiary PUFsecurity are highly credible. Experienced solution providers such as eMemory and PUFsecurity will still be the best choice now and moving into the post-quantum world.

14.Quantum-secure online shopping comes a step closer

by Martijn Boerkamp
https://physicsworld.com/a/quantum-secure-online-shopping-comes-a-step-closer/

Online shopping boomed during the pandemic, but it remains vulnerable to scams involving both buyers and sellers. Quantum communication could, in principle, add another layer of security, but verifying a transaction securely, rather than simply communicating it, requires a “signature” consisting of thousands of quantum bits (qubits) for a single bit of message.

For today’s noisy, imperfect quantum systems, that’s a very high bar, but researchers at China’s Nanjing University, Renmin University and the Beijing National Laboratory for Condensed Matter Physics found a way of lowering it. By using a mathematical technique called one-time universal hashing that generates shorter secure “keys”, the researchers substantially reduced the number of qubits required to verify an e-commerce transaction. They also considered different realistic source flaws based on a scheme that is independent of the measurement devices used, thereby avoiding the need for perfect signals to distribute the information.

From QKD to QDS

Quantum communication rests on the principle that anyone who tries to intercept a message encoded in quantum states will inevitably interfere with these states in a way that is easily detected. This principle is already used in quantum key distribution (QKD), but on its own, QKD cannot guarantee e-commerce security because it only provides a secure communication channel. It does not enforce other important e-commerce objectives such as integrity, authenticity or nonrepudiation (repudiation is where one party rejects the contract).

One possible way of fulfilling these other objectives involves a more complex method known as quantum digital security (QDS). This method uses the secure transmission of quantum states in QKD and the mathematics of information theory to generate unique keys for signing a contract and paying.

Ultra-secure protocol

The researchers’ QDS protocol involves three parties: a merchant, a client and a third party (TP). It begins with the merchant preparing two sequences of coherent quantum states, while the client and the TP

prepare one sequence of coherent states each. The merchant and client then send a state via a secure quantum channel to an intermediary, who performs an interference measurement and shares the outcome with them. The same process occurs between the merchant and the TP. These parallel processes enable the merchant to generate two keys that they use to create a signature for the contract via one-time universal hashing.

Once this occurs, the merchant sends the contract and the signature to the client. If the client agrees with the contract, they use their quantum state to generate a key in a similar way as the merchant and send this key to the TP. Similarly, the TP generates a key from their quantum state after receiving the contract and signature. Both the client and the TP can verify the signature by calculating the hash function and comparing their result to the signature. Payment can be made from the client to the TP if both verify the signature. If either of them cannot verify the signature, the contract is automatically aborted.

Quantum retailer

The researchers experimentally verified this protocol using optical fibres as quantum channels and a pulsed laser modulated in both phase and intensity to produce the quantum states for key generation. To eliminate the need for perfect devices, they characterized the source flaws of this system and combined the key generation process with a method called four-phase measurement device–independent QKD. This method uses the phase of the optical pulses at the intermediate interference measurement to obtain a secure key even if the intermediary that performs the measurement cannot be trusted.

To test the system's functionality, the team used it to sign a file containing 428 kB of data, which is approximately the size of an Amazon Web Services customer agreement. They were able to perform this signature 0.82 times per second, and the system worked even with the equivalent 100 km distance between the client and the merchant.

Team member Hua-Lei Yin, a quantum communications expert at Renmin, says the work shows it is possible to use non-repudiation features to perform e-commerce as efficiently and practically as private communications. The next step will be to demonstrate the technique in practical scenarios using real metropolitan quantum networks. "We hope to collaborate with more research groups to further develop quantum technology (including high-precision phase locking and phase tracking techniques) to improve the corresponding rates and transmission distances", he tells *Physics World*.

Qin Wang, an IT and networking expert at the Nanjing University of Posts and Telecommunications who was not involved in the research, says the quantum e-commerce scheme based on QDS offers enhanced security and practicality compared to corresponding classical schemes. The team's biggest achievement, she says, is to extend QDS to a useful scenario within e-commerce, thereby demonstrating its potential applications in daily life. She is, however, critical of Sagnac-type optical setup used in the experimental demonstration, which she says could be vulnerable to "Trojan horse" type hacks.

15.Cyber-attacks against Americans at all time high over past two years

by Mills Hayes
https://www.foxnews.com/tech/cyber-attacks-against-americans-all-time-high-over-past-two-years?utm_campaign=Oktopost-2024-01%20Advocate%20Posts&utm_content=Oktopost-linkedin&utm_medium=social&utm_source=linkedin

Cyber-attacks against Americans have hit an all-time high over the past two years, according to Checkpoint Software research. The Office of Government Accountability says the U.S. lacks adequate cybercrime data and monitoring, leaving the country less prepared to fight cybercrime.

Cyber criminals target education and research sectors the most because of their sensitive information and lack of adequate cyber security. Checkpoint Software Global Chief Information (CISO) Officer Pete Nicoletti says there was an increase in attacks on government and military in the 4th quarter of 2023.

“I think it's because of the ongoing conflicts that we're seeing. The two wars that the world is involved in,” Nicoletti said.

The Israel-Hamas war and the Russia-Ukraine war seem far away from Steele County, Minnesota. But Steele County Director of Information Technology Dave Purscell says our screens bring the war home.

“We’re at war, and literally against other countries that are attempting to do damage here," Purscell said. "We see a lot of activity against our firewalls that comes in from, you know, the big four, that'd be in Russia, China, Iran, and North Korea."

Purscell says cyber criminals target local governments because, "we have a lot of really important sensitive information. And the theory behind it is that we're not going to have the level of protection and security that a large organization like the federal or state government would have.”

The Bipartisan Infrastructure Deal of 2021 designates $1 billion for states and territories over the next 4 years. The Cybersecurity and Infrastructure Security Agency says states have to apply through the State and Local Cybersecurity Grant Program. Only South Dakota has not applied and received funds.

In Minnesota, the federal government has allocated $18 million in federal funds and $5.5 million in state matched funds from the Minnesota legislature. At least 80% of that has to go to local governments and at least 25% to rural communities.

CISO John Israel leads Minnesota IT Services executive branch cybersecurity teams and the Minnesota Cybersecurity Task Force. Israel says not every local government has adequate security measures. In September, the agency launched the Whole of State Cybersecurity Plan to provide and expand cybersecurity outreach to local governments statewide.

"Government entities, no matter how large or how small, collect and store manage a lot of data around presidents, about the people that they serve," Israel said. "Not only are they holding the data, ransom and hostage for payment, they're also trying to sell it on the black market.”

With 3,500 entities like school districts, local governments and tribal nations in Minnesota, Israel says the money goes fast.

Checkpoint software says attempted ransomware attacks on organizations rose 33% worldwide last year. About 1 in 20 organizations in the US fell victim to attempted ransomware attacks last year. On average, a business experiences over 1,158 cyberattacks a week.

"The criminal enterprise is actually growing in size. It's a multibillion-dollar industry. Some people think it's the third largest economy in the world after U.S. and China, the cybercriminal environment," Nicoletti said.

It’s not just the quantity of the cyberattacks that are increasing, but the quality. Nicoletti said the use of artificial intelligence has made phishing scams coming through email harder to spot.

16.Quantum Computing and Its Impact on Corporate Security and Privacy Compliance

by Medriva
https://medriva.com/business/quantum-computing-and-its-impact-on-corporate-security-and-privacy-compliance/

Quantum computing, the next frontier in information technology, is not just bringing new opportunities, but also posing significant challenges in corporate security and privacy compliance. Its arrival has been marked with a wave of excitement and concern in equal measure due to its potential to revolutionize various industries, including healthcare, and its ability to threaten traditional encryption methods. This article delves into the implications of quantum computing and the need for post-quantum cryptography to protect against its threats.

Understanding Quantum Computing and Its Threat to Traditional Encryption

Unlike classical computers which use bits representing either 0 or 1, quantum computers use qubits that can represent 0 and 1 simultaneously. This characteristic allows quantum computers to process information at an exponentially faster rate than classical computers. The increased processing power, while advantageous in many fields, poses a significant threat to traditional encryption methods and calls for a re-evaluation of data protection and security compliance.

Post-Quantum Cryptography: A Solution to Quantum Threats?

Post-quantum cryptography is seen as a potential solution to protect against quantum computing threats. It involves the creation of cryptographic systems that can withstand attacks from both classical and quantum computers. To address this, organizations are encouraged to create a quantum readiness roadmap, and follow three critical steps: discover, observe, and transform their cryptography. As artificial intelligence continues to evolve, organizations are urged to consider the impact of Generative Artificial Intelligence (GenAI) and adopt a holistic approach to IT and OT cybersecurity.

Quantum Computing and Industry Regulations

Regulation plays an essential role in managing the impact of quantum computing. In the EU and Canada, regulatory bodies are assessing the potential impacts of quantum computing on various sectors, including the insurance industry. Financial institutions are being encouraged to assess their quantum-readiness, with the development of rules, interpretation of legislation and regulation, and provision of regulatory approvals for certain types of transactions being key areas of focus.

Commercial Impact and Applications of Quantum Computing

Quantum computing has the potential to revolutionize various fields, from healthcare to financial services. Managed Service Providers (MSPs) have a critical role in helping small and medium-sized enterprises manage their cybersecurity needs effectively in this new era. They offer insights, strategies, and comprehensive IT and security services to mitigate risks and protect against cyber threats.

Quantum-Resistant Algorithms: A Paradigm Shift in Cybersecurity

The rise of quantum computing calls for a paradigm shift in cybersecurity. Quantum-resistant algorithms are being developed to safeguard data against the threat of quantum computers. Groundbreaking inventions in the field, like the quantum authentication and private data computing method patented by Quantum Computing Inc (QCi), offer promising solutions. This technology allows for processing and verifying information without sharing that information, effectively securing identity authentication, data mining, and digital assets in an untrusted environment.

In conclusion, while quantum computing offers unprecedented opportunities, it also raises concerns about corporate security and privacy compliance. Organizations need to adopt a proactive approach to quantum readiness, embracing the potential of post-quantum cryptography, and leveraging the expertise of MSPs. Regulation will play a key role in managing the impact of this technology, and quantum-resistant algorithms could be the future of cybersecurity.

17.India's Emergence Makes It A Critical Partner for The Western Quantum Ecosystem

by Matt Swayne
https://thequantuminsider.com/2024/01/19/indias-emergence-makes-it-a-critical-partner-for-the-western-quantum-ecosystem/

Recently, China and Russia announced that they successfully tested quantum communication over a distance of 3,800 kilometers, using secure keys transmitted by China's quantum satellite. Although no peer review research is — or is expected to be — made available, the satellite could give the nations a fully secure, unhackable link of communications.

Recently, the Eurasian Times is reporting that India — one of the BRICS (Brazil, Russia, India, China and South Africa) — was invited to join this quantum communication project. 'As last year's the Future Technologies forum, Russian President Vladimir Putin said he expected to discuss with "Indian partners, particularly in cutting-edge computing technology, data processing, storage, and transmission technologies."

The partnership would benefit the China-Russia project greatly. The country's quantum communication research is advanced — and these capabilities are growing.

While the invite appears to be rejected by India because of suspicions about China, according to the Eurasian Times, the news should be a reason for concern among the rapidly emerging quantum ecosystem in Western states. In the rapidly evolving world of quantum computing, more and deeper partnerships and collaborations with India would not just beneficial; they will be imperative.

As nations across the globe race to harness the transformative power of quantum technology, India stands out as a critical partner for the Western quantum ecosystem. The reasons for this are many, ranging from geopolitical significance to an abundant talent pool, technological prowess and more.

GEOPOLITICAL SIGNIFICANCE

India's strategic position in the global quantum community is as obvious as it is — seemingly — ignored. With its growing economy, political stability and strategic location, India is a pivotal player in global affairs. For Western countries, partnering with India in quantum computing could be not just a technological collaboration but a geopolitical strategy.

India would offer a counterbalance to other dominant forces in the quantum realm, particularly China, which is aggressively advancing its quantum capabilities. The West could serve as a counterbalance to China for India, as well.

An Indo-Western quantum alliance would foster a more diversified and balanced global quantum landscape, reducing the risk of a single-nation monopoly in this critical field.

A RICH TALENT POOL

India's greatest asset in the quantum journey is undoubtedly its talent. The country has a vast reservoir of young, talented, and highly skilled professionals in STEM fields. The Quantum Insider's Intelligence Platform lists more than 100 universities, government entities, research instiutions, companies and investors centered around India.

Indian universities and research institutions are churning out world-class scientists, engineers and programmers, many of whom are already contributing significantly to global tech giants and research labs. In the jigsaw puzzle of developing quantum supply chains, the biggest missing pieces for growing quantum startups is the lack of trained, skilled professionals.

By integrating this talent pool into the Western quantum ecosystem, there is an opportunity to accelerate innovation and development.

Additionally, such integration would provide Indian professionals with international exposure and opportunities, further enhancing their skills and contributions.

ENHANCING TECHNOLOGICAL CAPABILITIES

India has been making strides in quantum computing and related technologies.

The Indian government's significant investments in quantum research under initiatives like the "National Mission on Quantum Technologies and Applications (NM-QTA)" reflect a commitment to this field. By partnering with Western nations, India can leverage their advanced research facilities, funding, and expertise, leading to a synergistic relationship.

This collaboration would not only aid in the development of cutting-edge quantum technologies but also ensure that these advancements are grounded in diverse perspectives, leading to more robust and versatile solutions.

ECONOMIC IMPLICATIONS

The economic benefits of a robust Indo-Western partnership in quantum computing are immense.

Quantum technology is poised to revolutionize industries from cybersecurity to healthcare, finance, and logistics. By collaborating, both India and Western countries can tap into new markets, foster innovation, and drive economic growth. For India, it would mean an influx of foreign investment, job creation, and an opportunity to position itself as a leader in the quantum sector.

It's likely that India would have access to commercial opportunities in the West that they would not have in a Russia-China partnership.

CULTURAL AND EDUCATIONAL EXCHANGES

Such partnerships often extend beyond mere technological collaborations. And these collaborations could benefit quantum science, in general.

Increased Indo-Western collaborations could pave the way for cultural and educational exchanges, fostering a deeper understanding and appreciation of diverse viewpoints and practices. Joint research programs, academic exchanges, and collaborative projects between Indian and Western universities would enrich the educational experiences of students and researchers alike.

This cross-pollination of ideas is invaluable in a field as dynamic and interdisciplinary as quantum computing.

Perhaps, as a side note, Western universities, too, are facing cratering demographic issues that will affect enrollments. Indian talent could help shore up some of the damage of these shifting trends in student enrollment.

SECURITY AND STRATEGIC AUTONOMY

In a world increasingly defined by digital threats, quantum computing holds the key to unparalleled advancements in cybersecurity. An Indo-Western partnership in this domain would enhance collective security capabilities, particularly in encryption and data protection.

In addition, for India, such collaboration offers a path to strategic autonomy. By developing its quantum capabilities, India can ensure its national security, protect its data sovereignty, and reduce dependence on other nations for critical technologies.

INDIA'S QUANTUM STRENGTHS

When it comes to quantum strengths, India offers a buffet table of solid and innovative research output and entrepreneurship in many areas of the quantum industry and is leveraging quantum computers to explore key use cases. Just a few examples:

- **General Impact and Applications**: Quantum computing is seen as a key driver for advancements in various fields such as medications, machine learning, cybersecurity and climate change, with significant investment and initiatives like India's quantum mission aiming to develop a 50-qubit computer (Khan, Dalawai, & Nagachandan, 2020).

- **Enhancement of Artificial Intelligence**: The integration of quantum computing with AI is expected to significantly boost the capabilities of research activities globally (Mehta, Paharia, Singh, & Salman, 2019).

- **Renewable Energy Applications**: Research explores the utilization of quantum computing for industrial applications, particularly in the renewable energy sector (Rajawat et al., 2022).

- **Sustainable Development in IT Industry**: Quantum computing is recognized for its potential to revolutionize the Indian IT industry, contributing to sustainable development and employment generation (Chatterjee, 2018).

- **Quantum Information Theory and Quantum Computation**: Papers explore various aspects of quantum information theory and its applications in computation and communication (Pati &

Agrawal, 2012).

- **Healthcare Applications**: Quantum computing is being explored for applications in healthcare, such as diagnosing diabetic retinopathy more accurately and rapidly (S et al., 2022).

CHALLENGES AND DRAWBACKS

Obviously, the benefits of such a partnership are multifaceted — from geopolitical advantages to technological advancements, economic growth, and beyond. However, it may seem like a simplistic rundown of advantages. There are, of course, concerns. Adding more pieces to an already complex ecosystem offers just one more point of failure. Security risks for the broad Western quantum community could be exposed as well.

Understanding those concerns, there is a growing acknowledgement that the world stands on the brink of the development of quantum technology, for good and ill. The collaboration between India and Western nations could very well be the catalyst that propels us into a new era of technological prowess and innovation.

18.Summary of NATO's Quantum Technologies Strategy

https://www.nato.int/cps/en/natohq/official_texts_221777.htm

Introduction

1. Recent advancements in quantum technologies are bringing us closer to a profound shift for science and technology – one that will have far-reaching implications for our economies, security and defence. These technologies could revolutionise sensing; imaging; precise positioning, navigation and timing; communications; computing; modelling; simulation; and information science. Quantum technologies have potentially revolutionary and disruptive implications, which can degrade the Alliance's ability to deter and defend. Quantum technologies are therefore an element of strategic competition.

2. Quantum technologies have the potential to offer capabilities in computing, communications and situational awareness that are unparalleled to technology currently available to the Alliance and that could constitute a significant strategic advantage. However, quantum technologies can equally enable our strategic competitors and potential adversaries.

Strategic Vision: A Quantum-ready Alliance

3. To become a quantum-ready Alliance, NATO and Allies will foster the development of a secure, resilient and competitive quantum ecosystem that is able to respond to the fast pace of technological competition in the quantum industry. This requires coherence in investment, cooperation among Allies in technology development opportunities, development and protection of skilled workforce, and increased situational awareness as well as information sharing. It will also require development and deployment of critical enabling technologies that quantum technologies require. It is equally important to deter and defend our own systems and networks against quantum-enabled and other attacks.

4. To achieve the strategic ambition of becoming a quantum-ready Alliance, NATO and Allies will harness quantum technologies in support of the Alliance's core tasks, driving toward the following desired outcomes:

   - Allies and NATO have identified the most promising military and dual-use quantum applications, experiments, and integration of quantum technologies that meet defence planning and capability development requirements;
   - NATO has developed, adopted and implemented frameworks, policies and standards for both software and hardware to enhance interoperability;
   - Allies have cooperated in the development of quantum technologies with a view to maintain NATO's technological edge and Allies' abilities in the field;
   - NATO has identified, understood and capitalised on evolving quantum technologies advancements, including with enabling technologies and in convergence with other EDTs;
   - NATO has a Transatlantic Quantum Community to strategically engage with government, industry and academia from across our innovation ecosystems;
   - NATO has transitioned its cryptographic systems to quantum-safe cryptography;
   - Relevant quantum strategies, policies and action plans are dynamically updated and executed; and
   - Allies have become aware of, and act to prevent, on a voluntary basis, adversarial investments and interference into our quantum ecosystems, which can include, on a national basis, the examination of relevant supply chains.

5. Further, NATO will provide the leading transatlantic forum for quantum technologies in defence and security, helping to continuously build on our shared understanding, and leveraging the potential of quantum technologies while safeguarding against its adversarial use.

Fostering a Quantum-Ready Alliance

6. Allies and NATO must urgently accelerate the development of quantum technologies that can augment our capabilities, as well as prevent the formation of new capability gaps in a world where peer competitors adopt quantum technologies themselves. Given the dual-use nature of quantum technologies, this advantage can only be achieved if done in close cooperation with Allied quantum ecosystems. Allies and NATO must adopt a 'learn-by-doing' approach to integrating quantum technologies considerations in the implementation of our operational concepts, defence planning cycles, capability development cycles, and standardisation efforts.

7. As DIANA and the NATO Innovation Fund (NIF) become fully operational, their deep-tech activities will also inform NATO's strategic approach to quantum technologies and reinforce NATO's engagement with the Allied quantum ecosystem.

8. The convergence between quantum technologies and other EDTs brings important defence and security implications, and potential military applications and capabilities. Examples include using quantum sensors to improve space-based data collection and to enable positioning, navigation and timing capabilities without having to rely on Global Navigation Satellite Systems.

9. NATO recognises that one of the most critical resources in the pursuit of quantum advantage is talent, which will be a critical determinant of the Alliance's future trajectory in this domain. As

quantum technologies gain traction, so will the demand for experts with advanced degrees in the field.

Responsible Innovation

10. While quantum technologies have less obvious ethical implications relative to other EDTs such as AI, autonomy or biotechnology and human enhancement, Allies and NATO are nevertheless committed to instituting a responsible approach to quantum technologies innovation. This will cover three main areas: links to data privacy, anticipation of international norms development, and sustainability considerations.

11. NATO committees will also serve as platforms for Allies to exchange and cohere views on burgeoning quantum-related norms in international security, as they develop. Allies will exchange views at NATO, in line with this Strategy, and in light of other international fora.

12. To inform a comprehensive treatment of the risks and opportunities of the field of quantum technologies, the Data and AI Review Board (DARB) can offer its advice on the implications of developments in data and AI for quantum technologies.

A Transatlantic Quantum Community

13. A quantum-ready Alliance requires, first and foremost, a closer cooperation among Allies, and a resilient quantum ecosystem that extends beyond availability of appropriate funding. Successful scale up and adoption of quantum technologies also depends on availability of enabling technologies and effective links between new research breakthroughs and engineering methods. Quantum technologies are particularly reliant on enabling technologies. For example, quantum computers require precise metrology tools, secure manufacturing capabilities of specialised manufacturing and cryogenics.

14. End users and defence industry leaders play a crucial role in translating promising quantum technologies use cases into capabilities at scale. NATO is uniquely positioned to broker opportunities made possible by EDTs with industry, governments, and end users. The fast pace of development of quantum technologies calls for a coherent approach to this type of coordination and alignment among Allies, which will be provided by the establishment of a Transatlantic Quantum Community.

Protecting the Alliance from the Quantum Threat

15. Quantum technologies have a double-edged impact on cyber security and defence, benefitting both the defensive as well as the offensive side. If fully adopted, functional quantum technologies would allow private and public actors in the Alliance to better protect their data and communications in a way that is fast and reliable. A quantum-ready Alliance will be better able to detect and block potential incursions in cyberspace.

16. A functional quantum computer would also have the ability to break current cryptographic protocols.

17. Today, post-quantum cryptography is an important approach to secure communications against quantum-enabled attacks. In the future, further improvements could allow quantum key distribution to also contribute to secure communications.

18. Through NATO committees and bodies Allies can support each other, and the NATO Enterprise, in the development and implementation of post-quantum cryptography and quantum key distribution to enhance the quantum-resilience of our networks. NATO will continue to support research into the transition to quantum-safe communications across air, space, cyber, land and maritime do-

mains.

19. Strategic competitors and potential adversaries may also leverage disinformation opportunities within Allied societies by creating public distrust of the military use of quantum technologies. Allies will seek to prevent and counter any such efforts through the use of strategic communications. NATO will support Allies as required.

19.EnSilica adds Post Quantum Cryptography support to eSi-Crypto IP library

https://www.electronicsmedia.info/2024/01/15/post-quantum-cryptography-added-by-uks-ensilica/

EnSilica a leading chip maker of mixed-signal ASICs, has added a range of Post-Quantum Cryptography (PQC) accelerators to its eSi-Crypto range of hardware accelerator IP.

These cryptographic algorithms are developed to withstand cyber-attacks from quantum computers, and their launch makes EnSilica one of very few companies to offer advanced cryptographic accelerators to the market as licensable hardware IP cores. By implementing these in hardware cryptographic operations, such as encryption and decryption, can be performed faster, with lower-power and more securely than software-based implementations.

The first license for EnSilica's new QPC cores has now been granted to a major semiconductor company for target at a high performance 5nm networking chip.

Why PQC is essential:

Today's secure communications and financial transactions rely on public-key encryption techniques. These use maths problems a conventional computer cannot readily solve. However, advances in both quantum computing and artificial intelligence-based systems, which are backed by large datasets that need to be kept secured, means there is a real threat that cyber-attacks will break current standards.

As such, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) published its first draft standard for encryption algorithms capable of resisting quantum attacks in H2 last year. for the first of these cryptographic algorithms was published by the last year, with feedback completed in November.

In its 2023 announcement, the NIST mathematician Dustin Moody, who led the seven-year project to develop the algorithms said their creation meant "We're getting close to the light at the end of the tunnel, where people will have standards they can use in practice"

EnSilica's PQC accelerator IP:

EnSilica has added two new PQC accellerators to its eSi-Crypto range of IP:

- eSi-Dilithium is a hardware IP designed for accelerating the NIST FIPS 204 Module Lattice Digital Signature Algorithm called CRYSTALS Dilithium
- eSi-Kyber is a hardware IP designed for accelerating the NIST FIPS 203 Key Encapsulation Mechanism (KEM) called CRYSTALS Kyber.

Dilithium and Kyber algorithms are both part of the Cryptographic Suite for Algebraic Lattices (CRYSTALS) and are based on the computational difficulty of the Module Learning With Errors (MLWE) problem.

Additionally, the eSi-SHA3 has also been added to eSi-Crypto, this is a hardware IP designed for accelerating the NIST FIP 202 cryptographic hashing algorithms including SHA3 and SHAKE.

These add to and complement EnSilica's existing range of non-quantum resistant cryptography accelerators, which include ECC, EDCDA, RSA, AES, DES/3DES, SNOW3G, ChaCha20 and Poly1305 as well as a NIST compliant True Random number generator (TRNG). The cores are suitable for ASIC and FPGA usage and can be pre-configured to meet a range of throughputs and compatible with a range of AMBA buses including APB, AHB and AXI.

The timely adoption of PQC is driven by the concern that sensitive encrypted data harvested today, might one day be compromised once powerful quantum computers emerge. This is a critical security risk for governments safeguarding secrets and businesses handling sensitive and confidential information.

20.Encrypted mobiles with exclusive operating system — how Army is moving towards secure communication

by Smruti Deshpande
https://theprint.in/defence/encrypted-mobiles-with-exclusive-operating-system-how-army-is-moving-towards-secure-communication/1921412/

The Indian Army has created its own mobile operating system to be used on encrypted 5G enabled cellular phones for its officers to have a fool-proof communication system just like its internal landline network.

As part of the project, a total of 35,000 handsets for an end-to-end secure mobile ecosystem, will be configured in the next five months while 2,500 have already been rolled out.

Army sources said that mobile networks are prone to eavesdropping and thus information security of mobiles is at risk of being compromised.

An end-to-end secure mobile ecosystem, which is network agnostic, has been developed to provide secure communication with instant connectivity on the move. This leverages the potential of indigenous public cellular networks in the country. The ecosystem has 5G ready handsets using multi-tier encryption, the sources said.

The sets will be made available to almost all officers across the seven commands and other important appointments within the Army, a source said.

Under the project 'Secure Army Mobile Bharat Version' (SAMBHAV) ecosystem, the Army has indigenously developed cellular phones, which use dual-use infrastructure. The aim is to leverage the potential

of indigenous public cellular networks in the country.

SAMBHAV will be having multi layered encryption with Pan India Secure eco system. The phones will have an indigenous operating system with a multi-layered encryption, which has been developed in collaboration with the centres of excellence in both academia as well industry, including IIT-Madras.

The ecosystem will use 5G-ready handsets using multi-tier encryption. Encryption is a method used to secure communication. It scrambles data which can be read only by authorised parties using a secret code, enabling the mobile phones to ride on a commercial network with inherent security.

Until now, such phones did not exist and officers used regular phones for communication if not the secure landline network. Even though the phones will ride on the civilian infrastructure, they will be end-to-end encrypted by the Army.

The radio equipment operated by the Army operates in a range of 8-25 km, depending on the terrain. If it is a mountainous and high-altitude area, it may be limited to just 2-3 km.

The range, in this case, will be decided based on the coverage of a cell-phone tower, the source said, adding that this will further augment the Army's communication.

Currently, the Army uses landline connectivity using the Army Static Switched Communication Network (ASCON) IV. However, this is used for static communication and a need to have secure communication while on the go was felt, a second source in the security establishment said.

The source added that an experiment was done using the Code-Division Multiple Access (CDMA) technology more than a decade back, wherein Army personnel could speak to one another. However, the technology did not take off. Since these devices are encrypted, they are resistant to infiltration.

"There is a need for secure communication wherever the Army personnel go. Even though cell phones are carried by each personnel, these devices are susceptible to hacking and are not secure for communication to take place between Army personnel since it includes sensitive information," the source added.

21.Entrust Introduces First Commercially Available "Post Quantum Ready" PKI Platform

by Matt Swayne
https://thequantuminsider.com/2024/01/11/entrust-introduces-first-commercially-available-post-quantum-ready-pki-platform/

Entrust, a global leader in trusted payments, identities, and data, has announced the general availability of its Post-Quantum Ready PKI-as-a-Service (PKIaaS PQ) platform. With this launch, the company's cloud-based PKI as a Service offering now can provide both composite and pure quantum-safe certificate authority hierarchies, enabling customers to test or implement quantum-safe scenarios and infrastructure. This makes it the first commercially available platform of its type.

“Although the quantum threat is up to a decade away, we know the transition to quantum-safe algorithms won’t be just another crypto refresh cycle. To prepare, we need to move today’s public key cryptographic systems from their current state to new quantum safe cryptographic algorithms. This transition will be more complex than anything we’ve done in the past and will touch just about every piece of digital infrastructure and data we rely on today. Organizations should be looking at their Post Quantum (PQ) migration strategy now and implementing the tools and technology needed to test and migrate to quantum-safe security,” said Greg Wetmore, Vice President, Software Development at Entrust.

Backed by more than 25 years of Entrust PKI expertise and innovation, Entrust PKIaaS is a cloud-native service that simplifies PKI enterprise implementation and administration with pre-built, turnkey certificate use cases, including WSTEP, ACME, SCEP, and a broad range of mobile device management (MDM) solutions. The Entrust PKIaaS architecture also makes it simple for customers to scale on-demand by reducing on-premise services, applications, and software. It is designed to seamlessly integrate into existing workflows and applications, providing visibility, control, and automation of the environment from a single pane of glass, together with public SSL/TLS management via the cloud platform .

The addition of post-quantum cryptography, based on the NIST PQ draft standard algorithms, allows customers to issue quantum safe certificates in minutes, using both composite and pure quantum certificate authority hierarchies. This approach aligns with recommendations from global cybersecurity agencies such as the BSI in Germany and ANSSI in France, which recommend organizations test both hybrid and composite certificates as well as those based on pure quantum-safe algorithms.

“Leading national cybersecurity agencies around the world are recommending a hybrid approach to the transition to quantum safe data protection, with the use of hybrid or composite certificates to ensure protection in the form of classic and quantum-resistant cryptographic algorithms. With this launch, Entrust can support this transition and provide rapid, and scalable certificate generation and management. This approach also enhances an organization’s wider Zero Trust implementation and maturity by protecting their sensitive data from the “harvest now, decrypt later” threat, and ensuring their digital security infrastructure remains secure once the quantum threat is realized,” added Wetmore.

22.China claims it has cracked Apple AirDrop’s encryption to identify senders

by Juliana Liu and Hassan Tayir
https://edition.cnn.com/2024/01/10/tech/china-apple-airdrop-encryption-hnk-intl/index.html

A Chinese tech company has succeeded in cracking the encryption around Apple’s AirDrop wireless file sharing function to identify users of the popular feature, according to judicial authorities in Beijing.

The company, Wangshendongjian Technology, was able to help police track down people who used the service to send “inappropriate information” to passersby in the Beijing subway, the city’s Justice Bureau said in a Monday statement.

It had identified the senders’ mobile phone numbers and email addresses as part of an investigation following a complaint, the department said. Several suspects had been identified, it said, without giving details about the nature of the messages.

AirDrop has been blamed for nuisance messages received by some commuters on subways and buses in Chinese cities. The popular wireless file sharing function was also reportedly used by protesters to

spread anonymous messages critical of the Chinese government in the last few months of 2022.

Wangshendongjian Technology "broke through the technical difficulties of anonymous traceability through AirDrop," which "prevented the further spread of inappropriate remarks and potential bad influence," the department said.

CNN has reached out to Apple (AAPL) for comment.

According to international media, including The New York Times and Vice World News, some residents in China used AirDrop, which can be used only between Apple devices, to spread leaflets and images echoing slogans used in a rare protest against Chinese leader Xi Jinping in October 2022.

In 2019, AirDrop, which is effective only over short distances, was particularly popular among anti-government demonstrators in Hong Kong, who regularly used the feature to send colorful posters and artwork to subway passengers urging them to take part in protests.

In November 2022, shortly after the protest against Xi, Apple began to limit AirDrop sharing with non-contacts for devices in China, which made it harder for users to share files with people they didn't know. That feature was later expanded globally.

23.QuEra Computing Roadmap for Advanced Error-Corrected Quantum Computers, Pioneering The Next Frontier in Quantum Innovation

by Matt Swayne
https://thequantuminsider.com/2024/01/09/quera-computing-roadmap-for-advanced-error-corrected-quantum-computers-pioneering-the-next-frontier-in-quantum-innovation/?utm_source=newsletter&utm_medium=email&utm_term=2024-01-13&utm_campaign=TQI+Weekly+Newsletter+--+Entering+the+QuEra+Getting+Good+Chemistry+Plus+More+Quantum+News+Industry+Updates

QuEra Computing, the quantum computing trailblazer, today (09 Jan 2024) announced a bold strategic roadmap for a series of error-corrected quantum computers, starting in 2024 and culminating in a system with 100 logical error-corrected qubits. This announcement marks the ushering in of a new era in quantum computing and caps off a banner year for QuEra, which included breakthrough scientific results, substantial growth in its scientific and engineering teams, a new investment round, a significant increase in the availability of its Aquila platform on a major cloud platform, and more.

Quantum error correction is critical to fulfill the immense promise of quantum computers. This advanced technique addresses the inherent fragility of quantum states and the susceptibility of qubits to interference from their environment, which can lead to errors in quantum computations. By implementing error correction protocols, quantum computers can maintain the integrity of quantum information over longer periods, enabling them to perform complex calculations that are beyond the reach of classical computers. This not only enhances the reliability and scalability of quantum systems but also paves the way for groundbreaking advancements in fields ranging from materials science to drug discovery and optimiza-

tion problems. By providing the first commercial error-corrected system, QuEra is setting a new bar in performance and usability.

A THREE-YEAR QUANTUM ERROR-CORRECTION ROADMAP

QuEra's roadmap outlines a three-phase release of its revolutionary quantum computers:

- **2024:** Launching a quantum computer with 10 logical qubits, unique transversal gate capability, and over 256 physical qubits. Transversal gates are crucial in quantum computing for their ability to prevent error propagation across qubits, making them inherently error-resistant. They simplify quantum error correction by allowing errors to be corrected independently for each qubit. This system establishes the groundwork for error-corrected quantum computing. In addition, to assist in assessing and preparing algorithms for the era of error correction, QuEra will release a cloud-based logical qubit simulator in the first half of

- **2025:** an enhanced model with 30 logical error-corrected qubits with magic state distillation, supported by over 3000 physical Magic state distillation enables the implementation of a broader range of quantum gates with higher fidelity, allowing for the execution of non-Clifford gates, which are crucial for universal quantum.

- **2026:** Introduction of a third-generation QEC model with 100 logical qubits and over 10,000 physical qubits. This development, capable of deep logical circuits, will push quantum computing beyond the simulatability limit, ushering in a new era of discovery and innovation.

These advancements build upon the recent breakthrough published in Nature ("Logical quantum processor based on reconfigurable atom arrays", Bluvstein (Harvard) et al., Nature 2023), where a Harvard-led group, together with QuEra, MIT, NIST and the University of Maryland, reported the execution of complex algorithms with 48 logical qubits.

"With this product release plan, we are opening doors to a new world of computational possibilities," said Alex Keesling, CEO of QuEra Computing Inc. "We are excited to leverage all the building blocks developed in past years – qubit shuttling, transversal gates, high-fidelity 2- qubit gates – to deliver a world-leading system, allowing us to collaborate with global partners to explore the vast potential of quantum computing and drive innovation across various sectors."

CELEBRATING A YEAR OF SIGNIFICANT ACHIEVEMENT

This announcement comes on the heels of a breakthrough 2023 for QuEra, marked by significant progress on multiple fronts:

- Successfully completing a $30M Series A venture round early in the

- Expanding the public availability of QuEra's flagship 256-qubit Aquila system, available globally on a major cloud platform, from 10 to over 100 hours per week. Both commercial and academic customers enjoyed this increased availability, leading to several important results. Additionally, customers can now reserve blocks of machine time for exclusive access.

- Attracting top talent, significantly expanding the team to over 50 highly skilled scientists and engineers. Additionally, the company has added experienced and accomplished executives to its management team, positioning itself for accelerated growth and

- Scientists from Harvard, QuEra, MIT, UMD and NIST released a series of breakthrough scientific results. These advances provide critical building blocks and further cement QuEra's status as a leading quantum computing

"In a few years, the number of physical qubits will be less important to customers, and the focus will switch to logical error-corrected qubits", said Nate Gemelke, co-founder and CTO of QuEra. "Today, we are taking a major step in this critical transition from quantum experimentation to true quantum computing value."

CALLING DEVELOPERS, ENTERPRISES, AND HPC CENTERS

QuEra invites developers, enterprise customers, and High-Performance Computing (HPC) centers to engage with these groundbreaking capabilities. Developers are encouraged to adapt their software to take advantage of these new capabilities. Enterprises interested in exploring algorithms with logical qubits are invited to collaborate. HPC centers and national programs considering the purchase and on-premises deployment of these advanced computers are invited to register their interest. A new waitlist page at https://www.quera.com/waitlist is available for those interested in early access to these breakthrough capabilities.

24.Taiwan eyes 2027 for first local quantum computer

by Wu Po-hsuan and Jake Chung
https://www.taipeitimes.com/News/taiwan/archives/2024/01/07/2003811735

Taiwan aims to produce its first domestically developed quantum computer by 2027, the National Science and Technology Council (NSTC) said yesterday.

Quantum computing is the most anticipated next-stage development for raw computational power, said Luo Meng-fan (羅夢凡), head of the NSTC's Department of Natural Sciences and Sustainable Development.

The council has been working with the Ministry of Economic Affairs, Academia Sinica and other research organizations to realize a five-year, NT$8 billion (US$258.86 million) quantum technology plan that began in 2022, it said.

A Google study published in July last year showed how a random circuit sampling task that would have taken a classical supercomputer 47 years to complete was finished in just 6.18 seconds on the latest version of its Sycamore processor, which had been boosted to 70 quantum bit (qubits), Luo said.

In quantum computing, a random circuit sample task tests quantum computer performance by running random circuits and evaluating its capabilities and efficiency in solving complex problems.

With such powerful computational capabilities, security experts have warned that one day — dubbed "Q Day" — quantum computers would be able to crack codes protecting digital data, Luo said.

Measures to counter such development include quantum cryptography, such as quantum key distribution, he said.

However, quantum computers are still affected by high error rates, he said, adding that the technology needs another six years of research and development to reach maturity, when it could make a global impact.

That is why it is crucial for Taiwan to develop quantum computers to retain a foothold in critical technologies, he said.

The NSTC's collaboration with academia and other sectors would flesh out the component supply chain for building quantum computers and shorten the time necessary when transitioning the supply chain for commercial purposes, Luo said.

Taiwan is not alone in rushing to develop quantum computers, he said.

Taiwanese researchers are in talks with Finnish quantum computing hardware company IQM to establish testing platforms in Taiwan, he said.

Four cloud software computational platforms are utilizing the quantum cloud computation services offered by IBM, Amazon and other international companies, he added.

Academia Sinica is to provide some of its newly developed 5-qubit chips for trials at research facilities later this month, said Lee Chau-hwang (李超煌), executive secretary of the institute's Central Academic Advisory Committee.

Taiwan has only started developing quantum chipsets, but is closely monitoring increasing chipset yield rates, Lee said.

"Yield rates are key for mass production," he said.

25.KyberSlash attacks put quantum encryption projects at risk

by Bill Toulas
https://www.bleepingcomputer.com/news/security/kyberslash-attacks-put-quantum-encryption-projects-at-risk/

Multiple implementations of the Kyber key encapsulation mechanism for quantum-safe encryption, are vulnerable to a set of flaws collectively referred to as KyberSlash, which could allow the recovery of secret keys.

CRYSTALS-Kyber is the official implementation of the Kyber key encapsulation mechanism (KEM) for quantum-safe algorithm (QSA) and part of the CRYSTALS (Cryptographic Suite for Algebraic Lattices) suite of algorithms.

It is designed for general encryption and part of the National Institute of Standards and Technology (NIST) selection of algorithms designed to withstand attacks from quantum computers.

Some popular projects using implementations of Kyber are Mullvad VPN and Signal messenger. The latter announced last year that it adopted the CRYSTALS-Kyber KEM as an additional layer that attackers must break to compute the keys that protect the users' communications.

The KyberSlash flaws are timing-based attacks arising from how Kyber performs certain division operations in the decapsulation process, allowing attackers to analyze the execution time and derive secrets

that could compromise the encryption.

If a service implementing Kyber allows multiple operation requests towards the same key pair, an attacker can measure timing differences and gradually compute the secret key.

The problematic pieces of code that make the KyberSlash vulnerabilities (KyberSplash1 and KyberSplash2) were discovered by Goutam Tamvada, Karthikeyan Bhargavan, and Franziskus Kiefer - researchers at Cryspen, a provider of verification tools and mathematically proven software.

In a KyberSlash1 demo on a Raspberry Pi system, the researchers recovered Kyber's secret key from decryption timings in two out of three attempts.

Fixing effort underway

Cryspen analysts discovered KyberSlash1 late last November, and reported it to Kyber's developers, who pushed a patch for KyberSlash1 on December 1, 2023.

However, the fix wasn't labeled as a security issue, and it wasn't until December 15 that Cryspen took a more public approach and started informing impacted projects they needed to upgrade their Kyber implementations.

On December 30, KyberSlash2 was patched following its discovery and responsible reporting by Prasanna Ravi, a researcher at the Nanyang Technological University in Singapore, and Matthias Kannwischer, who works at the Quantum Safe Migration Center.

As of January 2, 2024, the list of projects below were identified as impacted by the issue and had the following fixing status:

- pq-crystals/kyber/ref – fully patched
- symbolicsoft/kyber-k2so – fully patched
- aws/aws-lc/crypto/kyber, main branch – fully patched
- zig/lib/std/crypto/kyber_d00.zig – fully patched
- liboqs/src/kem/kyber – patched only for KyberSlash1
- aws/aws-lc/crypto/kyber, fips-2022-11-02 branch – patched only for KyberSlash1
- randombit/botan – patched only for KyberSlash1
- mupq/pqm4/crypto_kem/kyber – patched only for KyberSlash1
- antontutoveanu/crystals-kyber-javascript – unpatched
- Argyle-Software/kyber – unpatched
- debian/src/liboqs/unstable/src/kem/kyber – unpatched
- kudelskisecurity/crystals-go – no patch yet
- PQClean/PQClean/crypto_kem/kyber/aarch64 – unpatched

- PQClean/PQClean/crypto_kem/kyber/clean – unpatched
-
- rustpq/pqcrypto/pqcrypto-kyber (used in Signal) – unpatched

Also, the following libraries are tagged as not impacted because they do not have divisions with secret inputs:

- boringssl/crypto/kyber
- filippo.io/mlkem768
- formosa-crypto/libjade/tree/main/src/crypto_kem/kyber/common/amd64/avx2
- formosa-crypto/libjade/tree/main/src/crypto_kem/kyber/common/amd64/ref
- pq-crystals/kyber/avx2
- pqclean/crypto_kem/kyber/avx2

The worst case scenario is leaking of the secret key but this doesn't mean that all projects using Kyber are vulnerable to key leaks.

The repercussions of KyberSlash depend on the Kyber implementation and can vary depending on the practical use cases and additional security measures.

For example, Mullvad says KyberSlash does not impact its VPN product because they're using unique key pairs for each new tunnel connection, making it impossible to perform a series of timing attacks against the same pair.

BleepingComputer has contacted Signal to learn about the actual impact of KyberSlash on its cryptography and users' communications, as well as the project's remediation plans, but a comment wasn't immediately available.

26.The need for post-quantum cryptography in the quantum decade

by Eric Sivertson
https://www.edn.com/the-need-for-post-quantum-cryptography-in-the-quantum-decade/

Cyber resilience has long been a key focus for industry leaders, but the stakes have been raised with the rapid acceleration of quantum computing. Quantum computing is a cutting-edge innovation that combines the power of computer science, physics, and mathematics to rapidly perform complex calculations outside the realm of classical computing. Expected to be commercialized by 2030, it offers incredible potential to further digitalize key industries and redefine the role technology plays in geopolitics. The possibilities of the post-quantum era cannot be understated.

While quantum computing can positively serve humanity in a myriad of ways, it also brings concerning cybersecurity threats. In turn, the U.S. government and security leaders have called for accelerated post-quantum cryptography (PQC) migration. President Biden signed the Quantum Computing Cyberse-

curity Preparedness Act after visiting IBM's quantum data center in October 2022. In addition, NIST, CISA, and NSA recently advised organizations to develop PQC readiness roadmaps.

The message is clear: *quantum-powered cyberattacks are of growing concern, and maintaining resilience in the face of this new threat is different than anything we've faced before.*

27.Quantum computing is taking on its biggest challenge: noise

by Michael Brooks
https://www.technologyreview.com/2024/01/04/1084783/quantum-computing-noise-google-ibm-microsoft/

In the past 20 years, hundreds of companies, including giants like Google, Microsoft, and IBM, have staked a claim in the rush to establish quantum computing. Investors have put in well over $5 billion so far. All this effort has just one purpose: creating the world's next big thing.

Quantum computers use the counterintuitive rules that govern matter at the atomic and subatomic level to process information in ways that are impossible with conventional, or "classical," computers. Experts suspect that this technology will be able to make an impact in fields as disparate as drug discovery, cryptography, finance, and supply-chain logistics.

The promise is certainly there, but so is the hype. In 2022, for instance, Haim Israel, managing director of research at Bank of America, declared that quantum computing will be "bigger than fire and bigger than all the revolutions that humanity has seen." Even among scientists, a slew of claims and vicious counterclaims have made it a hard field to assess.

Ultimately, though, assessing our progress in building useful quantum computers comes down to one central factor: whether we can handle the noise. The delicate nature of quantum systems makes them extremely vulnerable to the slightest disturbance, whether that's a stray photon created by heat, a random signal from the surrounding electronics, or a physical vibration. This noise wreaks havoc, generating errors or even stopping a quantum computation in its tracks. It doesn't matter how big your processor is, or what the killer applications might turn out to be: unless noise can be tamed, a quantum computer will never surpass what a classical computer can do.

For many years, researchers thought they might just have to make do with noisy circuitry, at least in the near term—and many hunted for applications that might do something useful with that limited capacity. The hunt hasn't gone particularly well, but that may not matter now. In the last couple of years, theoretical and experimental breakthroughs have enabled researchers to declare that the problem of noise might finally be on the ropes. A combination of hardware and software strategies is showing promise for suppressing, mitigating, and cleaning up quantum errors. It's not an especially elegant approach, but it does look as if it could work—and sooner than anyone expected.

"I'm seeing much more evidence being presented in defense of optimism," says Earl Campbell, vice president of quantum science at Riverlane, a quantum computing company based in Cambridge, UK.

Even the hard-line skeptics are being won over. University of Helsinki professor Sabrina Maniscalco, for example, researches the impact of noise on computations. A decade ago, she says, she was writing quantum computing off. "I thought there were really fundamental issues. I had no certainty that there

would be a way out," she says. Now, though, she is working on using quantum systems to design improved versions of light-activated cancer drugs that are effective at lower concentrations and can be activated by a less harmful form of light. She thinks the project is just two and a half years from success. For Maniscalco, the era of "quantum utility"—the point at which, for certain tasks, it makes sense to use a quantum rather than a classical processor—is almost upon us. "I'm actually quite confident about the fact that we will be entering the quantum utility era very soon," she says.

Putting qubits in the cloud

This breakthrough moment comes after more than a decade of creeping disappointment. Throughout the late 2000s and the early 2010s, researchers building and running real-world quantum computers found them to be far more problematic than the theorists had hoped.

To some people, these problems seemed insurmountable. But others, like Jay Gambetta, were unfazed.

A quiet-spoken Australian, Gambetta has a PhD in physics from Griffith University, on Australia's Gold Coast. He chose to go there in part because it allowed him to feed his surfing addiction. But in July 2004, he wrenched himself away and skipped off to the Northern Hemisphere to do research at Yale University on the quantum properties of light. Three years later (by which time he was an ex-surfer thanks to the chilly waters around New Haven), Gambetta moved even further north, to the University of Waterloo in Ontario, Canada. Then he learned that IBM wanted to get a little more hands-on with quantum computing. In 2011, Gambetta became one of the company's new hires.

IBM's quantum engineers had been busy building quantum versions of the classical computer's binary digit, or bit. In classical computers, the bit is an electronic switch, with two states to represent *0* and *1*. In quantum computers, things are less black and white. If isolated from noise, a quantum bit, or "qubit," can exist in a probabilistic combination of those two possible states, a bit like a coin in mid-toss. This property of qubits, along with their potential to be "entangled" with other qubits, is the key to the revolutionary possibilities of quantum computing.

A year after joining the company, Gambetta spotted a problem with IBM's qubits: everyone could see that they were getting pretty good. Whenever he met up with his fellow physicists at conferences, they would ask him to test out their latest ideas on IBM's qubits. Within a couple of years, Gambetta had begun to balk at the volume of requests. "I started thinking that this was insane—why should we just run experiments for physicists?" he recalls.

It occurred to him that his life might be easier if he could find a way for physicists to operate IBM's qubits for themselves—maybe via cloud computing. He mentioned it to his boss, and then he found himself with five minutes to pitch the idea to IBM's executives at a gathering in late 2014. The only question they asked was whether Gambetta was sure he could pull it off. "I said yes," he says. "I thought, how hard can it be?"

Very hard, it turned out, because IBM's executives told Gambetta he had to get it done quickly. "I wanted to spend two years doing it," he says. They gave him a year.

It was a daunting challenge: he barely knew what the cloud was back then. Fortunately, some of his colleagues did, and they were able to upgrade the team's remote access protocols—useful for tweaking the machine in the evening or on the weekend—to create a suite of interfaces that could be accessed from anywhere in the world. The world's first cloud-access quantum computer, built using five qubits, went live at midnight on May the 4th, 2016. The date, *Star Wars* Day, was chosen by nerds, for nerds. "I don't think anyone in upper management was aware of that," Gambetta says, laughing.

Not that upper management's reaction to the launch date was uppermost in his mind. Of far more concern, he says, was whether a system reflecting years of behind-the-scenes development work would

survive being hooked up to the real world. “We watched the first jobs come in. We could see them pinging on the quantum computer,” he says. “When it didn’t break, we started to relax.”

Cloud-based quantum computing was an instant hit. Seven thousand people signed up in the first week, and there were 22,000 registered users by the end of the month. Their ventures made it clear, however, that quantum computing had a big problem.

The field’s eventual aim is to have hundreds of thousands, if not millions, of qubits working together. But when it became possible for researchers to test out quantum computers with just a few qubits working together, many theory-based assumptions about how much noise they would generate turned out to be seriously off.

Some noise was always in the cards. Because they operate at temperatures above absolute zero, where thermal radiation is always present, everyone expected some random knocks to the qubits. But there were nonrandom knocks too. Changing temperatures in the control electronics created noise. Applying pulses of energy to put the qubits in the right states created noise. And worst of all, it turned out that sending a control signal to one qubit created noise in other, nearby qubits. “You’re manipulating a qubit and another one over there feels it,” says Michael Biercuk, director of the Quantum Control Laboratory at the University of Sydney in Australia.

By the time quantum algorithms were running on a dozen or so qubits, the performance was consistently shocking. In a 2022 assessment, Biercuk and others calculated the probability that an algorithm would run successfully before noise destroyed the information held in the qubits and forced the computation off track. If an algorithm with a known correct answer was run 30,000 times, say, the correct answer might be returned only three times.

Though disappointing, it was also educational. “People learned a lot about these machines by actually using them,” Biercuk says. “We found a lot of stuff that more or less nobody knew about—or they knew and had no idea what to do about it.”

Fixing the errors

Once they had recovered from this noisy slap, researchers began to rally. And they have now come up with a set of solutions that can work together to bring the noise under control.

Broadly speaking, solutions can be classed into three categories. The base layer is error suppression. This works through classical software and machine-learning algorithms, which continually analyze the behavior of the circuits and the qubits and then reconfigure the circuit design and the way instructions are given so that the information held in the qubits is better protected. This is one of the things that Biercuk’s company, Q-CTRL, works on; suppression, the company says, can make quantum algorithms 1,000 times more likely to produce a correct answer.

The next layer, error mitigation, uses the fact that not all errors cause a computation to fail; many of them will just steer the computation off track. By looking at the errors that noise creates in a particular system running a particular algorithm, researchers can apply a kind of “anti-noise” to the quantum circuit to reduce the chances of errors during the computation and in the output. This technique, something akin to the operation of noise-canceling headphones, is not a perfect fix. It relies, for instance, on running the algorithm multiple times, which increases the cost of operation, and the algorithm only estimates the noise. Nonetheless, it does a decent job of reducing errors in the final output, Gambetta says.

Helsinki-based Algorithmiq, where Maniscalco is CEO, has its own way of cleaning up noise after the computation is done. “It basically eliminates the noise in post-processing, like cleaning up the mess from the quantum computer,” Maniscalco says. So far, it seems to work at reasonably large scales.

On top of all that, there has been a growing roster of achievements in "quantum error correction," or QEC. Instead of holding a qubit's worth of information in one qubit, QEC encodes it in the quantum states of a set of qubits. A noise-induced error in any one of those is not as catastrophic as it would be if the information were held by a single qubit: by monitoring each of the additional qubits, it's possible to detect any change and correct it before the information becomes unusable.

Implementing QEC has long been considered one of the essential steps on the path to large-scale, noise-tolerant quantum computing—to machines that can achieve all the promise of the technology, such as the ability to crack popular encryption schemes. The trouble is, QEC uses a lot of overhead. The gold-standard error correction architecture, known as a surface code, requires at least 13 physical qubits to protect a single useful "logical" qubit. As you connect logical qubits together, that number balloons: a useful processor might require 1,000 physical qubits for every logical qubit.

There are now multiple reasons to be optimistic even about this, however. In July 2022, for instance, Google's researchers published a demonstration of a surface code in action where performance got better—not worse—when more qubits were connected together.

There have also been promising demonstrations of theoretical alternatives to surface codes. In August 2023, an IBM team that included Gambetta showed an error correction technique that could control the errors in a 12-qubit memory circuit using an extra 276 qubits, a big improvement over the thousands of extra qubits required by surface codes.

In September, two other teams demonstrated similar improvements with a fault-tolerant circuit called a CCZ gate, using superconducting circuitry and ion-trap processors.

That so many noise-handling techniques are flourishing is a huge deal—especially at a time when the notion that we might get something useful out of small-scale, noisy processors has turned out to be a bust.

Actual error correction is not yet happening on commercially available quantum processors (and is not generally implementable as a real-time process during computations). But Biercuk sees quantum computing as finally hitting its stride. "I think we're well on the way now," he says. "I don't see any fundamental issues at all."

And these innovations are happening alongside general improvements in hardware performance—meaning that there are ever fewer baseline errors in the functioning qubits—and an increase in the number of qubits on each processor, making bigger and more useful calculations possible. Biercuk says he is starting to see places where he might soon choose a quantum computer over the best-performing classical machines. Neither a classical nor a quantum computer can fully solve large-scale tasks like finding the optimal routes for a nationwide fleet of delivery trucks. But, Biercuk points out, accessing and running the best classical supercomputers costs a great deal of money—potentially more than accessing and running a quantum computer that might even give a slightly better solution.

"Look at what high-performance computing centers are doing on a daily basis," says Kuan Tan, CTO and cofounder of the Finland-based quantum computer provider IQM. "They're running power-hungry scientific calculations that are reachable [by] quantum computers that will consume much less power." A quantum computer doesn't have to be a better computer than any other kind of machine to attract paying customers, Tan says. It just has to be comparable in performance and cheaper to run. He expects we'll achieve that quantum energy advantage in the next three to five years.

28.SK, Thales collaborate on 5G post-quantum cryptography

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/sk-thales-collaborate-on-5g-post-quantum-cryptography/

As 5G networks roll out and cryptographic standards evolve, SK Telecom (SKT), the largest mobile operator in Korea, and Thales, leader in digital security, have partnered to successfully test advanced quantum-resistant cryptography.

Based on 5G standalone network and 5G SIM technology, the solution aims at encrypting and decrypting subscriber identity in a secure way to protect user privacy from future quantum threats. This cryptography achievement is already crucial today as it protects subscribers against potential "record now, decrypt later" attacks. It represents a major step forward since it allows to safeguard subscribers' identities via a regular commercial telecom network.

The innovation upgrades the cryptography used to anonymize the user digital identity on the 5G network. Indeed, the user identity on a 5G network is concealed and secured on the device side thanks to the 5G SIM. The security mechanisms involve cryptographic algorithms designed to resist attacks from future quantum computers, providing a level of security that is considered robust in the post-quantum era.

The National Institute of Standards and Technology (NIST) has been leading an initiative to standardize post-quantum cryptographic algorithms, and **SKT and Thales have used the Crystals-Kyber one for this successful real condition trial**. These post-quantum secure algorithms are being developed to withstand attacks from both classical and quantum computers.

"This collaboration between SKT and Thales highlights our commitment to staying ahead of the curve in terms of cybersecurity and ensuring the safety of our customers' data. PQC provides enhanced security through the use of cryptographic algorithms that are thought to be secure against quantum computer attacks. Going forward, we will combine PQC SIM with our additional quantum expertise to achieve end-to-end quantum-safe communications," said Yu Takki, Vice President and Head of Infra Technology Office of SKT.

"As quantum computers have the potential to break certain existing cryptographic algorithms, there is an emerging need to transition to cryptographic algorithms believed to be secure against quantum attacks. For 5G networks, Thales started to invest on cryptographic algorithms that are quantum-resistant to enhance continued communications security and privacy for users," said Eva Rudin, SVP Mobile Connectivity and Solutions at Thales.

29.Side-Channel Attack Protection for Quantum Safe Cryptography

by Bart Stevens
https://semiengineering.com/side-channel-attack-protection-for-quantum-safe-cryptography/

A recent Reuters Special Report discussed the race between the US and China to protect digital assets and communications from the potential threat posed by quantum computers. Cryptographically relevant quantum computers, those that are powerful enough to crack existing public key-based encryption methods, could compromise military, economic, and personal information across the globe. While the race is on to harness the benefits of quantum computers in science, industry, and medical applications, so too is the race to protect our data against attacks from quantum computers.

Quantum Defen5e (QD5), a Canadian cybersecurity firm, predicts a critical moment known as "Q-day" around 2025, when quantum computers may render current encryption useless. As we start a new year, 2025 suddenly doesn't seem that far away, and we can no doubt expect the conversation around Quantum Safe Cryptography to continue the momentum that we have seen recently.

In August 2023, NIST published the first three draft standards for general-purpose encryption algorithms that can resist attack by quantum computers. These draft standards are FIPS 203 for ML-KEM (based on the CRYSTALS-Kyber algorithm), FIPS 204 for ML-DSA (based on the CRYSTALS-Dilithium algorithm), and FIPS 205 for SLH-DSA (based on the SPHINCS+ algorithm).

Deep learning-based side-channel analysis methods have already shown a protected CRYSTALS-Kyber hardware implementation to be vulnerable to profiling attacks (as detailed here and here) leading to successful key recovery. Similarly, side-channel attacks on CRYSTALS-Dilithium have been attempted. In this blog, I'll be covering side-channel attacks in the context of Quantum Safe Cryptography as robust side-channel attack protection will remain an important security consideration in the quantum era.

The individual components of ML-KEM and ML-DSA are relatively straightforward to protect against side-channel attacks with countermeasures such as Boolean and arithmetic masking. However, in both, the full algorithms are more difficult and expensive to protect than the individual components due to their constructions. The first point is that both algorithms frequently switch between operations that require Boolean masking and operations that require arithmetic masking, so costly mask conversion algorithms are required. Furthermore, mask conversions have a long history of being tricky to implement securely; in the past it was always a good idea to avoid mask conversions altogether. This is not possible for ML-KEM and ML-DSA.

Protecting ML-KEM

ML-KEM, like many other KEM proposal algorithms in NIST's PQC competition, uses the Fujisaki-Okamoto (FO) transform to construct an IND-CCA2 secure KEM from a simpler, IND-CPA secure public key encryption scheme. This includes a re-encryption step after decryption in order to protect against chosen ciphertext attacks. Unfortunately, it was discovered that the re-encryption can leak information about the private key (source) despite not using the private key. ML-KEM is based on the Module Learning With Errors (MLWE) problems, which contains a certain error correcting capability. MLWE is not an error correcting code but can correct some errors. After decrypting a faulty ciphertext, the information about what kind of error is present in the underlying message or whether the error was corrected depends on the private key used for decryption and can leak during the re-encryption step. Combining such observations from multiple faulty ciphertexts then allows mathematical deductions of the private key.

This is like message-recovery attacks on generic public-key encryption, so it's not entirely new, but it significantly increases the attack surface for the ML-KEM decapsulation routine. Furthermore, it has emerged that profiled attacks on the FO transform are significantly easier for KEMs based on the FO transform as the profiling can be done on the encapsulation operation. Thus, powerful machine learning attacks (either classical template attacks or more novel deep learning attacks) have quickly become the most popular side-channel attack against ML-KEM. More classical side-channel attacks such as differ-

ential power analysis (DPA) are still relevant, but the profiled attacks are more powerful without the usual difficulty to perform profiling.

Protecting ML-DSA

ML-DSA, on the other hand, introduces novel difficulty for side-channel security assessments. Since the runtime of the algorithm is inherently probabilistic and message dependent without a fixed upper bound, security labs need to decide how to deal with the runtime differences. Small runtime differences are well known from some countermeasures (e.g., dummy cycles and clock jitter) and methods to deal with them are well established. Similarly, key recovery attacks that target specific intermediate values have well established alignment methods to ensure maximum efficiency for minimal certification cost. However, more generic methods such as TVLA struggle with the more pronounced probabilistic runtimes, and methods to rule out false positives from unlucky runtime outliers need to be studied more carefully. It is not clear that simply discarding outlier traces to avoid false positives doesn't risk discarding real leakage. Initially, a combination of increased code review and layered evaluation will need to be followed, but further research may clarify under what conditions discarding outliers during the test is perfectly safe and lead to simpler test procedures.

Implementing side-channel attack protection is an important component for establishing an overall Quantum Safe design. The Rambus Quantum Safe IP Portfolio offers solutions that combine Quantum Safe Cryptography and DPA resistance. The Rambus QSE-IP-86 Quantum Safe Engine is a standalone cryptographic core that supports the NIST draft standards FIPS 203 ML-KEM and FIPS 204 ML-DSA. A DPA version of the core includes DPA-resistant cryptographic accelerators. Offering a secure basis for hardware-level security, the RT-65x and RT-66x Root of Trust families offer Quantum Safe Cryptography and protect against a wide range of hardware and software attacks through state-of-the-art side-channel attack countermeasures and anti-tamper security techniques.

30.UAE, Saudi Arabia, and Qatar spearheading quantum computing development in the Middle East

by Inga Stevens and Kate McGinley
https://www.zawya.com/en/press-release/events-and-conferences/uae-saudi-arabia-and-qatar-spearheading-quantum-computing-development-in-the-middle-east-kiyw42vn

The rapid advancement of quantum computing has ignited a fierce race for the next era of computing innovation globally and across the Middle East, according to new research from Frost & Sullivan. While the United States and China hold the top positions in quantum computing and cryptography development, the growing prominence of quantum computing in the Middle East region will be discussed in detail at Intersec 2024, which takes place from 16-18 January 2024 at the Dubai World Trade Centre (DWTC).

Quantum computing has the potential to revolutionise cybersecurity by improving secure communication with advanced encryption. Yet, it also challenges current encryption methods, so preparing for this quantum era is vital to protect data from new risks.

Although quantum computing is still in its early stages, it will likely impact fields like scientific research,

cryptography, finance, supply chains, logistics, and drug discovery as it develops further.

Speaking ahead of the Cyber Security Conference at Intersec 2024, Rajarshi Dhar, Principal Consultant, Security, Frost & Sullivan, said: “Quantum computing represents a revolutionary leap in computational power, promising to transform industries. While still nascent, this technology holds immense potential for solving complex problems faster and more efficiently than classical computers. As we continue to advance our understanding and capabilities in quantum computing, it is clear that this field will play a pivotal role in shaping the future of science, technology, and society at large.”

Frost & Sullivan's analysis predicts a significant surge in the quantum cryptography market over the next five years, with more than half of the revenue expected to come from businesses, followed by the government and defence sectors.

“This growth is propelled by the imminent threat posed by the commercialisation of quantum computers, making current security and cryptography outdated. Upgrading security systems is crucial, requiring future-proof cryptography capable of withstanding both quantum and sophisticated attacks,” **Dhar added.**

Although the United States holds the top position in quantum computing and cryptography development, China is following closely behind and is anticipated to impact technological advancement significantly in the future.

Meanwhile, the UAE has also been in a race for quantum computing and quantum cryptography development with its own Quantum Research Centre and UAE’s institutes working towards productisation. In September 2023, the Technology Innovation Institute developed cryptography estimators that evaluate the security of Post-Quantum Cryptography (PQC) schemes.

Similarly, Qatar and Saudi Arabia are making substantial steps in the quantum computing space with a US$ 10 million investment from the Qatari government towards the Qatar Centre for Quantum Computing. Saudi Arabia recognises the need to establish the Quantum Computing Council for Saudi Arabia.

The implications of quantum computing will be discussed in detail at the two-day Intersec 2024 Cyber Security Conference, which will gather experts, thought leaders, practitioners, and innovators as they collectively chart the course for cyber security excellence in the years to come.

Other notable regional and international speakers include His Excellency Dr. Mohamed Al Kuwaiti, Head of Cyber Security, UAE Government; Fadhel Al Marri, Security Systems Officer, Dubai Electronic Security Center; Craig Jones, Director – Cybercrime, Interpol, Singapore; and Sergi Marcen, Secretary of Telecommunications & Digital Transformation, Government of Catalonia, Spain.

Grant Tuchten, Portfolio Director at Intersec organiser Messe Frankfurt Middle East, said: "The Cyber Security Conference allows the industry to deepen its understanding of cyber security risks and enhance cooperation among stakeholders to counter these risks effectively. Intersec will also host world-leading cyber security exhibitors within the in{:cyber} Pavilion, including Fortinet, Moro Hub, Alpha Data, and ManageEngine.”

The Intersec 2024 in{:cyber} Pavilion features the Hack Arena, a three-day challenge for Middle East cybersecurity experts hosted by Malcrove CTF.ae. Participants demonstrate skills in web exploitation, digital forensics, cryptography, exploit development, and reverse engineering. Also, the Intersec Innovators Arena (IIA), powered by Unipreneur Inc, offers startups a platform to showcase products to potential investors.

Workshops within the pavilion include the ITU-led Scenario Based Exercise, analysing attack scenarios, and the Table Top Exercise, simulating cyber-attacks on financial institutions.

Intersec's 25th edition, held under the patronage of His Highness Sheikh Mansoor Bin Mohammed bin Rashid Al Maktoum, marks a quarter-century of innovation in security tech. With 1,000 exhibitors from 60 nations and 45,000 trade visitors, the event is a global hub for security, safety, and fire protection industries.

31.How Can SMEs Prepare for The Quantum Computing Era?

by Matt Swayne
https://thequantuminsider.com/2024/01/03/how-can-smes-prepare-for-the-quantum-computing-era/

What happens when the world's small, extremely powerful businesses meet science's small, utterly transformative technologies?

The opportunities — and the challenges — are mind blowing.

The idea of quantum computing, once relegated to academic circles and science fiction novels, has now migrated to the tech media, and now is headed toward mainstream media outlets, like 60 Minutes. While it's impossible to predict how technologies — or if technologies — are adopted, it's evident that quantum technology is here, and it seems poised to revolutionize everything from drug discovery to materials science.

And as the headlines trumpet the quantum exploits of tech giants like Google and IBM, there's a critical question for the often unrecognized backbone of the global economy: **Do small and medium-sized enterprises (SMEs) need to pay attention to the emerging quantum technology industry?**

The answer is yes. While the immediate impacts of full-blown quantum computing may be felt first by larger players, **the underlying principles and tools offer SMEs opportunities waiting to be explored and possibilities waiting to be unleashed.** Understanding quantum technology can put SME owners, executives and employees ahead of the curve, preparing your business to ride the wave of innovation when it crests.

So, why exactly should SMEs get in on the quantum revolution? Here are a few reasons:

1. The Possibility of Quantum Advantage: Solving Problems Previously Untouchable

Classical computers have limitations, like struggling with complex simulations or optimization problems. Quantum computers, however, offer the potential to harness the unique physics of the quantum world to achieve speed ups in these areas. This could one day translate to:

- **Faster drug discovery and materials science:** Imagine designing new life-saving medications or innovative materials in a fraction of the time, accelerating your R&D and giving SMEs a competitive edge.
- **Enhanced logistics and optimization:** Quantum algorithms can optimize complex delivery routes or financial portfolios with unprecedented accuracy, saving businesses time and money while maximizing efficiency.

- **Unbreakable encryption:** This is a opportunity and a threat. SMEs need to prepare for the post-quantum cryptography era by understanding the security benefits and challenges of quantum computing, ensuring their data remains safe in the new quantum landscape.

2. Accessing the Quantum Ecosystem: From Early Adopters to Collaborators

The quantum ecosystem is booming, with a growing network of startups, research institutions, and even cloud giants offering access to their quantum computing resources. This means SMEs can:

- **Tap into early adopter programs:** Be among the first to experiment with quantum computing solutions, gaining valuable insights and shaping the future of this technology.
- **Partner with quantum startups:** Collaborate with nimble, innovative companies to develop custom quantum solutions for your specific business needs, or to explore how quantum might effect the business landscape.
- **Leverage cloud-based quantum computing:** Access powerful quantum processors through the cloud, without the hefty upfront investment in hardware, making the technology more accessible than ever.

3. Future-Proofing Your Business: Preparing for the Quantum Revolution

While the full effects of the quantum revolution still appears to be a few years away, the initial waves of this transformative change has already hit the shore. Learning about quantum technology now positions your business as:

- **A talent magnet:** Attract and retain top talent by fostering a culture of innovation and curiosity, showcasing your commitment to cutting-edge technologies. By the way, attracting quantum-ready talent takes time, which is another reason to add this to the overall quantum business strategy.
- **A thought leader:** Position yourself as an industry leader by staying ahead of the curve on quantum trends, building trust and credibility with customers and partners.
- **A future-ready organization:** By familiarizing yourself with quantum concepts and applications, you ensure your business is adaptable and equipped to thrive in the transformative quantum era.

4. Dodge Competitive Bullets, Attain Early Adoption Advantages

- **Outmaneuver the competition:** SMEs have stiff competition from new, aggressive startups and older, established players. Early adopters of quantum computing may help SMEs prepare for competition in the quantum era.
- **Early Adopter Advantage:** Right now, many — some studies point to around 80 percent — businesses, both small, large and in-between, are not even thinking about quantum computing and other quantum technologies. SMEs that adopt early could likely attain competitive advantages even against bigger businesses that fail to adopt the technology.
- **Enter New Markets:** As we indicated, quantum computing have the potential to change how SMEs do business and alter their competitive landscapes, but this technology may also open up new markets and reveal new opportunities. Be better prepared for when these currently un-

known unknowns appear.

So, how can SMEs start their quantum journey? Here are some practical steps:

- **Follow quantum news and thought leaders:** Start by subscribing to resources — here comes an unrepentant TQI plug — like The Quantum Insider (https://app.thequantuminsider.com/) and following experts on social media, staying informed about the latest developments.
- **Attend webinars and workshops:** Numerous online and offline events cater to beginners, offering introductions to quantum concepts and potential applications for business.
- **Enroll in online courses:** Several universities and platforms offer beginner-friendly online courses on quantum computing and its implications.
- **Connect with local quantum communities:** Look for quantum startups, research labs, or industry groups in your area to foster local connections and collaboration opportunities.

The future of quantum technology is becoming more visible, and the opportunities for SMEs are vast. By taking the initiative to understand and engage with this transformative technology now, you can ensure your business navigates the coming quantum wave with confidence and success. Remember, in the quantum race, the early birds may not catch the worm, but they'll certainly be best positioned to build their nest amidst the inevitable technological revolution.