Crypto News

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

July 01, 2024

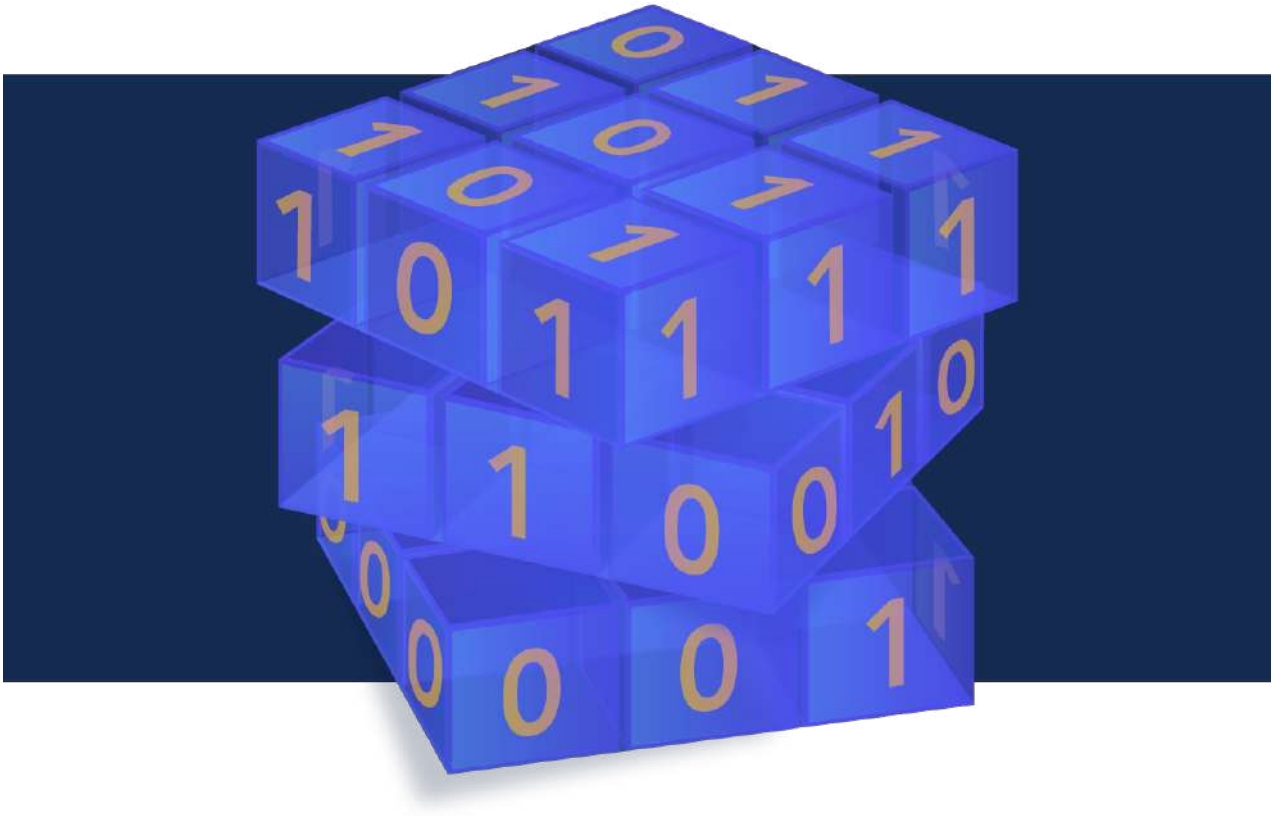


TABLE OF CONTENTS

Editorial

Dear Readers,

Here is your eagerly awaited monthly Crypto News, compiled for you by Dhananjoy.

This month, the compilation is truly international, with news from China (**4**), India (**10**), a historical review explaining how crypto helped end apartheid in South Africa (**26**), news from Estonia (**25**) and many others. Since France has been in the news recently and will be again towards the end of the month (have you ever heard about Olympic games?), we can also look at their Quantum program in (**3**), learn about their progress in quantum computing (**6**), or see how a combination of QKD and PQC might be a great solution in (**22**).

Maybe the most useful article, giving advice on why, when and how to get ready against the Quantum Threat is (**33**), with an interview of Dustin Moody from NIST. This is truly information from the source. And interesting one as well.

If you are into the fundamentals of quantum versus classical information theory and are ready for a harder read, (**2**), or equivalently (**32**), should be your choice. We learn that quantum could offer a great solution for some tasks, even if classical computation is found to be easy (i.e., no hard problem to rely on). A bit on the hard side, but fascinating.

In any case, you can also make your own choice. Enjoy your reading!

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security-Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA and it is compiled by Dhananjoy Dey.

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.The Interplay of AI, Cybersecurity and Quantum Computing

by James Dargan
https://thequantuminsider.com/2024/06/29/the-interplay-of-ai-cybersecurity-quantum-computing/

At the Tech.eu Summit in London, Dr. Ken Urquhart, Global Vice-President of 5G/Edge/Satellite at Zscaler, and Steve Brierley, Founder and CEO of Riverlane, discussed the critical intersection of artificial intelligence (AI), cybersecurity and quantum computing. Moderated by Duygu Oktem Clark, Managing Partner at DO Venture Partners, the talk underlined both the challenges and opportunities these technologies present.

AI & Its Limitations in Cybersecurity

Urquhart opened the discussion by addressing the limitations of AI in cybersecurity.

"AI, as we apply it today, involves algorithms that are interpretable and useful for cyber defense," he said. However, he pointed out that current AI technologies, such as neural networks and large language models, come with issues like statistical variability and hallucinations, where the AI "makes things up that may not be true."

Urquhart explained that these statistical models could become less accurate over time, adding: "You need to be thoughtful about how you apply AI because it can give less accurate answers if asked the same question twice in a row over a span of hours or days."

Quantum Computing's Potential & Challenges

Brierley shared his thoughts into the advancements in quantum computing and its implications for cybersecurity. He noted that while today's quantum computers are "extremely error-prone" and capable of only about 100 to 1000 operations before failure, significant progress is being made with quantum error correction.

"Quantum error correction is a layer that sits on top of the physical qubits and corrects errors in real-time," Brierley explained.

This development is crucial for achieving cryptographically relevant quantum computing capabilities.

"2023 and 2024 have been pivotal years as we crossed the threshold in various qubit modalities, making error correction viable," he said. Brierley projected that within the next two to three years, we could see quantum computers performing up to a million operations, surpassing what classical computers can simulate.

Ethical & Security Considerations

As AI and quantum computing advance, ethical and security challenges emerge. Urquhart stressed the importance of understanding AI's current limitations.

"We are on a journey with artificial intelligence. It does not think; it is a collection of statistical outcomes," he stated. Urquhart warned against over-reliance on AI for critical decisions, as its current form can lead

to significant errors.

Brierley added that quantum computing has the potential to revolutionize industries, particularly in simulating molecular dynamics and chemical interactions.

“Quantum computers can replace time-consuming lab experiments with simulations, transforming industries like drug discovery and material science,” he said.

Collaboration for a Secure Digital Future

Both experts agreed on the necessity of collaboration among academia, industry and government to harness these technologies responsibly. Brierley called attention to the importance of a coordinated effort, likening it to a “Manhattan-scale project” to build the world’s most powerful quantum computers. “We need effective collaboration across sectors to ensure the technology benefits society,” he said.

Urquhart echoed this sentiment, giving emphasis to the role of commercial entities in driving innovation and the government’s role in providing a regulatory and funding environment.

“The machinery is there; we just need the will to engage and make it run,” he remarked.

The Future of Quantum & Cybersecurity

Looking ahead, both Urquhart and Brierley stressed the urgency of preparing for the impact of quantum computing on cybersecurity.

“Quantum computing will break most encryption at some point,” Urquhart warned, urging businesses to act now to mitigate future risks.

Brierley concluded: “Quantum computers are not just faster computers; they represent a massive step forward for specific problems, and their potential for both good and bad is immense.”

The discussion underscored the transformative potential of AI and quantum computing while cautioning against complacency. As these technologies evolve, proactive collaboration and ethical considerations will be paramount in shaping a secure digital future.

2.Cryptographers Are Discovering New Rules for Quantum Encryption

by Ben Brubaker
https://www.wired.com/story/cryptographers-are-discovering-new-rules-for-quantum-encryption/

Researchers have proved that secure quantum encryption is possible in a world without hard problems, establishing a new foundation for what is needed to keep information secure.

Say you want to send a private message, cast a secret vote, or sign a document securely. If you do any of these tasks on a computer, you’re relying on encryption to keep your data safe. That encryption needs to withstand attacks from code breakers with their own computers, so modern encryption methods rely on assumptions about what mathematical problems are hard for computers to solve.

But as cryptographers laid the mathematical foundations for this approach to information security in the 1980s, a few researchers discovered that computational hardness wasn't the only way to safeguard secrets. Quantum theory, originally developed to understand the physics of atoms, turned out to have deep connections to information and cryptography. Researchers found ways to base the security of a few specific cryptographic tasks directly on the laws of physics. But these tasks were strange outliers—for all others, there seemed to be no alternative to the classical computational approach.

By the end of the millennium, quantum cryptography researchers thought that was the end of the story. But in just the past few years, the field has undergone another seismic shift.

"There's been this rearrangement of what we believe is possible with quantum cryptography," said Henry Yuen, a quantum information theorist at Columbia University.

In a string of recent papers, researchers have shown that most cryptographic tasks could still be accomplished securely even in hypothetical worlds where practically all computation is easy. All that matters is the difficulty of a special computational problem about quantum theory itself.

"The assumptions you need can be way, way, way weaker," said Fermi Ma, a quantum cryptographer at the Simons Institute for the Theory of Computing in Berkeley, California. "This is giving us new insights into computational hardness itself."

This Message Will Self-Destruct

The story begins in the late 1960s, when a physics graduate student named Stephen Wiesner started thinking about the destructive nature of measurement in quantum theory. Measure any system governed by the rules of quantum physics, and you'll alter the quantum state that mathematically describes its configuration. This quantum measurement disturbance was a hindrance for most physicists. Wiesner, who took an unorthodox information-centric view of quantum theory, wondered whether it could be made useful. Perhaps it could serve as a form of built-in tamper protection for sensitive data.

But Wiesner's ideas were too far ahead of their time, and he left academia after graduate school. Fortunately, he'd discussed his ideas with his friend and fellow physicist Charles Bennett, who unsuccessfully tried to interest others in the subject for a decade. Finally, in 1979, Bennett met the computer scientist Gilles Brassard while swimming off the coast of Puerto Rico during a conference. Together, they wrote a groundbreaking paper describing a new approach to an important cryptographic task. Their protocol was based on quantum measurement disturbance, and needed no assumptions about the difficulty of any computational problems.

"The very nature of quantum information seems somewhat cryptographic," Ma said.

Bennett and Brassard's breakthrough made researchers optimistic that similar quantum tricks could yield perfect security for other cryptographic tasks. Researchers focused mainly on a task called bit commitment, which is useful on its own and is also a key component of most advanced cryptographic protocols.

To understand the basic idea behind bit commitment, imagine a two-player game in which you must make a secret decision that later gets revealed. One way to do this is to write the decision down on a slip of paper and put it in a sealed envelope. That way, you can't change your decision later on, and your opponent can't prematurely peek at the result.

Now imagine you're playing the same game online. To make cheating impossible, you need to seal the decision in a sort of digital envelope that neither player can open alone. That's where cryptography comes in. In 1981, the pioneering computer scientist Manuel Blum constructed the first bit commitment

protocol—a way to build effectively unhackable envelopes out of hard computational problems.

But how hard is hard? Researchers in the field of computational complexity theory study many different kinds of hard problems, and not all of them are useful for cryptographers. Bit commitment and all other cryptographic protocols rely on problems in a class that complexity theorists call "NP," whose defining feature is that it's easy to check whether a candidate solution is correct.

Unfortunately, researchers haven't been able to prove that any NP problems are truly hard. There could still be some clever undiscovered procedure, or algorithm, for solving even the ones that seem hardest. If there is, then all of classical cryptography would break.

Such considerations animated the search for quantum-based security guarantees. But in 1997, two papers proved that bit commitment schemes could never be completely secure if they were based solely on the laws of quantum physics. The papers implied that some kind of computational hardness would be necessary for almost all cryptographic tasks.

That was the last word on the theoretical foundations of quantum bit commitments for nearly 25 years. Then, in 2021, a paper by a graduate student named William Kretschmer prompted researchers to confront a question that nobody had thought to ask. Computational hardness was clearly necessary for bit commitments and most other forms of cryptography, but precisely what kind of hardness?

The answer would turn out to be weirder than anybody had anticipated.

Consulting Oracles

The 2021 paper came out of Kretschmer's struggle to understand a specific version of a problem that sounds conceptually straightforward: How hard is it to distinguish, or discriminate between, two quantum states that look superficially similar? Kretschmer, who's now a postdoctoral researcher at the Simons Institute, was initially interested in the problem for reasons that had nothing to do with bit commitment.

"Cryptography was not even on my radar," he said.

The discrimination problem was interesting in part because it wasn't even clear how to describe it using familiar mathematical language. Complexity theorists traditionally study problems with different possible inputs represented by strings of bits, or 0s and 1s. For the problem of decomposing large numbers into their prime factors, for instance, this string represents the number to be factored.

Even after researchers started studying how quantum physics might be harnessed for computation, they continued to focus on such "classical-input" problems. Typical quantum algorithms start with an ordinary classical bit string and then process it using quantum trickery. But in "quantum-input" problems like Kretschmer's, the inputs aren't bit strings—they're quantum states that are as easily disrupted by computation as by measurement.

"The language with which we've described quantum computations in traditional complexity theory can't directly talk about these problems," Yuen said.

At first, Kretschmer thought he just needed to translate the problem into more standard language, but he couldn't figure out how. So he did what complexity theorists often do when they're desperate: He turned to an oracle.

In complexity theory, the term "oracle" refers to a hypothetical device that can solve a specific problem instantly. A computer with access to an oracle might be able to solve other problems more easily by

consulting the oracle as an intermediate step in an algorithm. Of course, oracles don't actually exist in the real world, but studying them helps complexity theorists understand the relationships between the difficulty levels of different problems.

Kretschmer wondered what kind of oracle could make it easy to distinguish two quantum states—the so-called state-discrimination problem. He decided to start with a special oracle that would boost the power of normal quantum algorithms, the ones that use quantum tricks to solve problems with classical bit string inputs. Such algorithms can solve some problems too hard for classical ones, like factoring large numbers, but they're not omnipotent—many other problems lie beyond their reach.

Access to Kretschmer's oracle would enable such algorithms to solve certain classical-input problems too hard for real quantum computers. Kretschmer assumed that it would be overkill, but to his surprise, he proved that the state-discrimination problem could still stump these souped-up quantum algorithms.

"I was really fascinated by William's paper," said Luowen Qian, a graduate student studying cryptography at Boston University. "I actually thought it had to be wrong, because it's so counterintuitive."

Qian, Yuen, and others soon proved that if Kretschmer's state discrimination problem really was hard, secure quantum bit commitment schemes would be possible. That would in turn imply security for a slew of more advanced cryptographic protocols. The scope of quantum cryptography was far broader than researchers in the 1990s had realized, and it all came down to the hardness of one problem.

How Hard Could It Be?

Kretschmer's result came with one big caveat—to make the proof work, he had to rely on an unusual oracle that only quantum algorithms could consult. Perhaps a more familiar oracle would make his state discrimination problem easy, and therefore make secure quantum bit commitments impossible? In 2022, Kretschmer and Qian began working together to see what they could prove about an oracle everybody could understand: one that could solve any NP problem instantaneously. In a world with such oracles, all classical cryptography would be impossible.

Kretschmer soon realized that the state discrimination problem was mathematically related to a superficially different problem in quantum complexity theory, and he enlisted the help of two experts in the area, the complexity theorists Avishay Tal and Makrand Sinha. "William was really like a manager, and we were contractors," Tal said.

Working together, the four researchers quickly proved that Kretschmer's state discrimination problem could still be intractable even for computers that could call on this NP oracle. That means that practically all of quantum cryptography could remain secure even if every problem underpinning classical cryptography turned out to be easy. Classical cryptography and quantum cryptography increasingly seemed like two entirely separate worlds.

The result caught Ma's attention, and he began to wonder just how far he could push the line of work that Kretschmer had initiated. Could quantum cryptography remain secure even with more outlandish oracles—ones that could instantly solve computational problems far harder than those in NP? "Problems in NP are not the hardest classical problems one can think about," said Dakshita Khurana, a cryptographer at the University of Illinois, Urbana-Champaign. "There's hardness beyond that."

Ma began brainstorming how best to approach that question, together with Alex Lombardi, a cryptographer at Princeton University, and John Wright, a quantum computing researcher at the University of California, Berkeley. "It was just so fascinating and so mind-bending that I was immediately hooked," Wright said.

After thinking about the question for a while and getting nowhere, Ma suggested that they consider the most extreme case possible: an oracle that could instantly solve any computational problem with classical inputs. That would include all the problems complexity theorists have traditionally studied, even those known to be unsolvable in the real world.

“It sounded a little bit insane to me,” Lombardi said.

But the question turned out to be remarkably fruitful. After working on it for nearly a year, they finally published a striking result. No algorithm allowed to consult that all-powerful oracle exactly once can distinguish the two quantum states, as is required to undermine a quantum bit commitment scheme.

Limiting algorithms to a single query is less of a constraint than it may sound, because quantum algorithms can effectively ask the oracle to solve multiple problems simultaneously by exploiting the phenomenon called superposition. Algorithms that can make multiple queries sequentially could be more powerful, because they can use the oracle’s answers to previous queries to decide what to ask next. Whether these algorithms are similarly limited remains an open question.

Ma, Lombardi, and Wright’s paper was also significant for another reason. While the three researchers were wrestling with their problem, they realized it was closely linked to a major open problem posed 16 years earlier by the complexity theorist Scott Aaronson and the mathematician Greg Kuperberg, about the difficulty of transforming one quantum state into another. The new paper was the first significant step toward settling that question.

“It’s a very strong result and also a very surprising result,” said Tomoyuki Morimae, a quantum cryptography researcher at the Yukawa Institute for Theoretical Physics in Kyoto.

The string of recent results suggests that the innocuous-sounding problem of distinguishing two quantum states is not just hard, but almost inconceivably hard—far beyond the reach of normal quantum algorithms and even more exotic ones. That’s good news for cryptography, but it also has broader implications for computational problems whose inputs are quantum states. Traditional complexity theory seems unable to address these problems. Truly understanding them might require a radically new theoretical framework.

“It feels like there’s something fundamentally different about how quantum information behaves,” said Andrea Coladangelo, a quantum cryptographer at the University of Washington. “It’s bound to have connections that are also beyond cryptography.”

3.French National Quantum Report – June 2024

by Matt Swayne
https://thequantuminsider.com/2024/06/28/french-national-quantum-report-june-2024/

EXECUTIVE SUMMARY

Traditionally, business activity slows down, however, not in quantum and certainly not in France. French policymakers, business leaders and scientists joined the broader quantum community in a burst of activity in June. In one significant milestone, neutral quantum computing pioneer Pasqal announced it has crossed the critical 1000-qubit threshold. In fact, the company trapped more than 1110 atoms within

approximately 2000 traps. On the capital markets side of the ecosystem, C12, a French spin-off of the Physics Laboratory of the École Normale Supérieure in Paris, closed an 18 million Euro funding round. Alliances, collaborations and partnerships are the ties that bind the French quantum community with the global quantum ecosystem. This month French policymakers continue to make progress – including a deal inked with the United States to promote cooperation on emerging technologies such as quantum. Meanwhile, the whole ecosystem is busy with building networks within the nation, as well as fostering connections worldwide. Overall, the month has been a productive beginning to the summer months in quantum for France. What follows is a non-exhaustive summary of some of the French quantum ecosystems achievements and milestones.

POLICY

France and the United States recognize the importance of promoting transatlantic academic research collaboration in critical and emerging technologies, to include, quantum, AI, and biotechnology.

BUSINESS

Pack Quantique Île-de-France: a new project supported by the Ile-de-France region and its partners to federate the French quantum ecosystem and support the scaling-up of quantum computing around algorithm parallelization. As part of the Pack Quantique (PAQ), initiated at the end of 2020, the Île-de-France Region (Paris Region) has decided to provide €2 million in support for the AQADOC project, led by Welinq, EDF, Pasqal and Quandela. This is the world's first consortium to bring together quantum computer manufacturers, end-users and a quantum machine interconnect manufacturer to explore the benefits of parallelizing algorithms to enable the scaling-up of quantum computing.

L'Etat is launching a communication campaign, with several French companies, to make quantum computing more concrete. A way to promote and justify its stated ambitions in this area.

IBM and Pasqal, as leaders in superconducting circuit and neutral atom-based quantum computers respectively, announced their intent to partner to develop a common approach to quantum-centric supercomputing and promoting application research in chemistry and materials science. IBM and Pasqal will work with leading institutions in high-performance computing to establish the foundations for quantum-centric supercomputing — the integration of quantum computing with advanced classical computing to create the next generation of supercomputers.

C12, a French spin-off of the Physics Laboratory of the École Normale Supérieure in Paris and a pioneer in the development of a carbon nanotube-based universal quantum computer, announces the closing of its second financing round of €18 million. This marks a new step in C12's development to accelerate the design of quantum processors. It brings together leading investors, Varsity Capital, EIC Fund, and Verve Ventures, as well as historical investors including 360 Capital, Bpifrance through its Digital Venture fund, and BNP Paribas Développement.

A pioneering 100+ qubit quantum processing unit (QPU), acquired by GENCI (Grand Équipement National de Calcul Intensif), was delivered at TGCC, the CEA computing centre, announce the three partners. As the first QPU to be delivered to a third party by Pasqal, a global leader in neutral atom quantum computing, this significant milestone is part of the broader High-Performance Computer and Quantum Simulator hybrid (HPCQS) project, co-funded by the European HPC Joint Undertaking, along with GENCI, in the field of HQI (France Hybrid HPC Quantum Initiative), supported by the France2030 investment programme.

Quandela, the European-based quantum computing provider, inaugurates its first manufacturing pilot line for high-performance photonic qubit devices, aiming to accelerate the deployment of error-corrected quantum computers. Following the successful opening of its first quantum computer factory in June

2023, which already enabled the delivery of two quantum computers to industrial customers, this new production site underscores Quandela's commitment to industrial scaling and innovation in the quantum computing sector.

As part of the ParisRegionQCI project, a consortium of market players, university researchers and startups set out to prove the feasibility of quantum key distribution using existing terrestrial fiber networks — and succeeded. Thomas Rivera, a Research Project Manager at Orange with a PhD in optics and photonics, coordinated the project. He reflects on this major step forward for French quantum communications.

RESEARCH

Pasqal, a global leader in neutral-atom quantum computing, today announced a significant technological milestone: the successful loading of over 1000 atoms in a single shot within their quantum computing setup. This breakthrough marks a crucial step in Pasqal's progress towards quantum advantage and scalable quantum processors.

Artificial intelligence (AI) is advancing at breakneck pace, with the EU struggling to keep up with the regulatory, competitive and economic implications. But quantum computing is one technology which has the potential to speed up the development of AI where the EU might have the upper hand. According to data analysed by Science|Business, France, the Netherlands, and Austria are hotspots in the field. Quantum computing is promising to transform a range of other technologies, including AI, and leading organisations in these three countries are preparing for the new wave. The French National Centre of Scientific Research (CNRS) tops the pack, winning around €40 million from Horizon 2020 and Horizon Europe, followed by the Technical University of Delft and the The French Alternative Energies and Atomic Energy Commission.

The French Navy took delivery of its first serial-produced, quantum-technology sensor this year, a quantum gravimeter used for mapping the seabed, the head of the country's defense innovation agency AID said. Future uses of such sensors could be for navigation or detecting enemy submarines.

EDUCATION AND EVENTS

Following the open elections in 2023, the Academy of Sciences has elected 18 new members. A session will be held in their honor under the Dome of the Institut de France, on Tuesday, June 4, 2024.

France Quantum 2024, the premier French quantum computing conference, brought together top experts and thought leaders for a live roundtable discussion on the current state and future potential of this revolutionary technology. One expert panel featured Fanny Bouton (OVHcloud) Quantum Lead & Startup Program Leader, Jean Senellart (Quandela) Chief Product Officer, and Dr. Laurent Guiraud (ColibriTD) Co-Founder & Head of Quantum Computing R&D.

4.Chinese Leadership Says Country Needs an Innovative Leap Forward in Quantum, Emerging Technologies

by Matt Swayne

https://thequantuminsider.com/2024/06/27/chinese-leadership-says-country-needs-an-innovative-leap-forward-in-quantum-emerging-technologies/

A recent deep dive into research output published in The Economist shows the China has become a global research powerhouse, including vast leaps in scientific investigations into quantum computing and artificial intelligence (AI). Converting that scientific knowledge into business innovation is where the country stumbles — and Chinese leadership recently passed out national failing grades in that subject.

China's leader, Xi Jinping, acknowledged significant challenges in the country's quest to move from being a research leader to a global tech powerhouse, reports the Business Insider. Speaking at a national conference in Beijing, Xi admitted that China's innovation capabilities are "relatively weak" despite the country's overall strength in science and technology.

Xi's remarks highlighted the urgent need for advancing in technology, which he termed the "main battlefield of international competition."

He candidly noted that, although China has made considerable progress in science and technology, its original innovation remains lacking.

"Although the country's science and technology development has made great progress, its original innovation capabilities are still relatively weak," Xi said, as reported by the Business Insider.

During his speech, Xi emphasized the importance of innovation 55 times, BI notes, particularly in areas such as AI, quantum technology, biotechnology and new energy. Despite recognizing the country's achievements, Xi also stressed that technological breakthroughs are too scattered across various sectors and companies, leading to a "low degree of organization and coordination."

He also mentioned that the nation's scientists were "overburdened," likely a reference to the non-research duties of scientists.

Measuring Innovation

Innovation is a factor that is difficult to measure scientifically, but a preliminary look at The Quantum Insider's Intelligence Platform shows that, at least according to some innovation indicators of the quantum industry, Xi may be onto something. Chinese universities and research institutions lead, or are among the global leaders, in research output — as measured by the number of scientific papers that are published — across the quantum technological landscape, such as quantum computing, quantum sensing and quantum communication.

However, there is scant evidence of significant quantum partnerships within China or internationally, compared to what is becoming a global approach to quantum innovation that relies on building interdisciplinary ecosystems with members who are spread across academia, government and business. For example, a cursory examination of a sample of research papers on the platform show that while academic-commercial and cross-institutional authorship is somewhat common among the quantum research output of non-Chinese nations, China's research papers tend to be authored by scientists from a single institution without partners in commercial organizations or, often, other academic institutions.

Similarly, while global efforts are focused on developing quantum use cases — practical applications of quantum computing and quantum technologies in solving complex problems — there are few examples of this work going on in China. Of course, these results could be attributed to a range of other causes, including a lack of publicity and communication, rather than a lack of effort in China.

Perhaps more symbolically, both Alibaba and Baidu, once banners for China's quantum innovation and

market reform entrepreneurism, shut down their quantum programs and donated the equipment to university efforts.

Self-Reliance

A key theme of Xi's address was self-reliance, BI reports, especially in light of escalating tensions with Western nations.

"The scientific and technological revolution and the wrestling between superpowers are intertwined," Xi said, without directly naming the United States. He pointed out that China needs to address the issue of "some key core technologies" being controlled by other countries.

Xi's comments come as the United States considers expanding sanctions on Chinese chip firms linked to Huawei and continues to block the sale of advanced semiconductors crucial for artificial intelligence development, BI reports. Recently, the U.S. Treasury Department labeled China a "country of concern" and proposed new regulations to limit international investments in technologies with potential national security risks. The United States — joined with many other western nations — also announced restricting technology exports to many Chinese emerging tech firms, including China's biggest quantum computer companies and their subsidiaries.

In addition to these geopolitical challenges, Xi called out domestic issues within China's tech and science sectors. Just as other country's face struggles finding the right talent for an increasingly more technical workforce, Xi acknowledged a shortage of skilled manpower and top talent, alongside heavy nonacademic burdens faced by researchers, such as excessive bureaucracy in publishing papers and securing resources.

Xi called for improved incentive systems, including better awards for scientific achievements and a more equitable wage system for employees and researchers.

Some experts see that solving the academic-entrepreneurial disconnect in China will require more than a few incentives and policy tweaks, but are systemic results of Xi's own economic reforms.

Martin Miszerak, a visiting lecturer at Renmin Business School, Renmin University, Beijing, wrote last September that the government has essentially squashed the entrepreneurial business model in China, according to his piece the East Asia Forum, which publishes analysis and research on economic, political, social and international issues in the Asia-Pacific region. Miszerak writes: "Before November 2020, those companies were very different from most of China's large private companies. Their business model at that time could be described as 'entrepreneurial' — completely private, backed by world-class venture capital and guided by entrepreneurial leaders dedicated to shareholder value maximisation. This entrepreneurial business model has now been extinguished. Instead, these firms must align with other large private Chinese companies which tend to be intertwined with the state. This ensures significant state influence over the private sector."

While the United States enjoys a tech boom driven by giants like OpenAI, Nvidia, Amazon and Microsoft, China's tech sector faces mounting pressure. According to Business Insider, China's top five tech companies have lost approximately $1.3 trillion in market value since 2021, leading to increased demands on workers from industry bosses.

The Chinese government's focus on artificial intelligence development has been particularly intense. Business Insider previously reported that a Microsoft study indicated China-linked social media accounts intended to use AI-generated content to influence U.S. elections.

Xi's speech underscores his ambition for China not just to participate but to dominate the global tech

landscape.

“We must bolster our sense of urgency. We must go further with our efforts to innovate,” Xi said. “To occupy the commanding heights of science and tech competition and future development.”

5.Lastwall Unveils First-of-its-Kind Quantum Resilient Product: Quantum Shield

by Lastwall
https://www.prnewswire.com/news-releases/lastwall-unveils-first-of-its-kind-quantum-resilient-product-quantum-shield-302182703.html

Lastwall, a leading cybersecurity solutions provider of highly secure, identity-centric, and quantum resilient technologies, today announced the launch of Quantum Shield, a first-of-its-kind quantum resilient product that protects conventional network infrastructures with the latest quantum cryptographic standards. Lastwall is backed by Blue Bear Capital, BlueWing Ventures, and 18 West Capital Partners.

In light of identity-related incidents continuing to dominate today's headlines, concerns about emerging 'Steal-Now-Decrypt-Later' campaigns targeting all sectors — from defense to critical infrastructure — are at an all-time high. Most pressing is the impending threat of a cryptographically relevant quantum computer, Q-Day, which has the capability to break the majority of modern encryptions. With the National Institute of Standards and Technology (NIST) set to release updated guidance on approved quantum-resilient algorithms within the next 30-60 days, the widespread adoption of quantum-resistant solutions is more important than ever.

Leveraging a NIST pre-approved algorithm that integrates Post-Quantum Cryptography (PQC) into the Transport Layer Security (TLS) layer of network traffic, Lastwall's Quantum Shield significantly enhances security. Designed to be crypto-agile, Quantum Shield can rapidly update with minimal configuration changes to accommodate newly approved algorithms as NIST standards evolve.

"Quantum cryptographic resilience is central to our product stack, with our identity platform built around this as a core defensive principle," stated Karl Holmqvist, Founder and CEO, Lastwall. "Having successfully provided transport layer resilience to our internal and client security operations, we now aim to make it accessible to all organizations through our Quantum Shield offering. The urgency to protect critical data intensifies as the acceleration of quantum computational capabilities advances. Having a fast, easy-to-deploy solution that has been thoroughly vetted will be helpful to those who recognize the need to act now.”

Lastwall's Quantum Shield is the industry's first mass-deployable, quantum-safe TLS terminator and load balancer. Featuring an easy one-click installation, Quantum Shield seamlessly replaces existing TLS terminators and load balancers, delivering an immediate and critical foundation of quantum resilience for network data and communications. As a quantum-hardened network endpoint, Quantum Shield meets the highest and most rigorous standards of security, compliance, and efficiency, effectively managing network traffic and enabling the protection of conventional network infrastructure with the latest quantum cryptographic standards.

"We have been working with Lastwall since 2017, and its platform has consistently evolved to meet our increasing needs," stated John Chen, Chief Information Officer, Defense Innovation Unit, U.S. Department of Defense. "Lastwall's focus on Zero Trust and secure by design components, coupled with its

ability to exceed compliance requirements, provides significant advantages in addressing today's dynamic threat landscape. We're excited to continue leveraging their advanced capabilities, especially at a time when quantum resilience is becoming increasingly critical."

"Quantum Shield is timely and essential. With NIST soon releasing quantum-resilient algorithm guidelines, Lastwall is not just meeting but anticipating the rigorous security needs of global industries." stated Carolin Funk, Partner, Blue Bear Capital. "We are proud to back their mission to build and deploy advanced digital defense solutions, ensuring that critical data and IT infrastructure is secured against emerging cybersecurity threats."

6.Pasqal Reports Loading More Than 1000 Atoms In Quantum Processor

by Matt Swayne
https://thequantuminsider.com/2024/06/25/pasqal-reports-loading-more-than-1000-atoms-in-quantum-processor/?utm_source=newsletter&utm_medium=email&utm_term=2024-06-29&utm_campaign=TQI+Weekly+Newsletter+--+1+000-Plus+Qubits+Centered+on+Excellence+Plus+More+Quantum+News+Industry+Updates

Pasqal, a global leader in neutral-atom quantum computing, today announced a significant technological milestone: the successful loading of over 1000 atoms in a single shot within their quantum computing setup. This breakthrough marks a crucial step in Pasqal's progress towards quantum advantage and scalable quantum processors.

In a major technological advancement for the quantum computing industry, Pascal has trapped more than 1110 atoms within approximately 2000 traps, demonstrating the feasibility of large-scale neutral atom quantum computing. In Pasqal's quantum computing architecture, these atoms are confined and manipulated using electromagnetic fields. The internal energy states of these atoms serve as the quantum states of the qubits, which are manipulated to perform quantum operations and execute quantum algorithms.

This successful trapping of single rubidium atoms in large arrays of optical tweezers, comprising up to 2088 sites, within a cryogenic environment at a temperature of 6 K represents one of Pasqal's latest feats in quantum computing. This achievement involves innovative optical designs that combine ultra-high-vacuum-compatible microscope objectives at room temperature with windowless thermal shields, ensuring efficient trapping at cryogenic temperatures. In an industry first, Pasqal demonstrated atom-by-atom rearrangement of an 828-atom target array using moving optical tweezers controlled by a field-programmable gate array (FPGA).

This large-scale trapping of atoms is essential for building scalable quantum processors capable of solving complex problems efficiently. As the number of qubits increases, so does the computational power and the range of problems that can be tackled using quantum algorithms. The ability to trap and manipulate over 1000 atoms represents a significant advancement towards creating quantum processors that can address problems currently beyond the abilities of classical computers.

"Achieving the 1000-atom milestone illustrates the great scalability of Pasqal's quantum processors," said Loic Henriet, Co-CEO of Pasqal. "These innovative results will fuel the design of future hardware products with enhanced computational power."

This milestone aligns with Pasqal's strategic roadmap, which emphasizes the development of quantum computers with over 1000 qubits, progressing towards 10000 qubits by the 2026-2027 horizon. The roadmap highlights Pasqal's commitment to advancing hardware capabilities and exploring high-impact business use cases in collaboration with Fortune 500 companies.

7.LG Uplus launches VPN service using post-quantum cryptography

https://www.telecompaper.com/news/lg-uplus-launches-vpn-service-using-post-quantum-cryptography--1504458

LG Uplus has introduced the 'U+ PQC-VPN' virtual private network solution featuring post-quantum cryptography (PQC) technology for corporate customers. PQC refers to encryption algorithms that are difficult to hack, even with quantum computers that operate faster than supercomputers. The operator said the new service is also the first of its kind to be issued a 'Security Function Confirmation' by the National Intelligence Service.

LG Uplus's PQC-VPN offers eight types of solutions tailored to different internet bandwidths, ranging from 500 Mbps to 36 Gbps, allowing companies to adopt the solution according to their specific needs. Additionally, the operator provides a 24-hour monitoring service through its security operation centre. With this new solution, companies can utilise PQC-encrypted communication by simply adding a single device to their existing internet setup, without requiring extensive construction. This offers an alternative to subscribing to additional dedicated line services.

The operator said the service is expected to be beneficial for companies that need to exchange encrypted data between their headquarters and branches nationwide. It is particularly advantageous for public institutions, financial institutions, hospitals, and other organisations that handle sensitive customer information. Previously, in 2021, LG Uplus invested in CryptoLab and has been developing solutions applying PQC algorithms. In 2022, the operator said it became the first domestic telecom company to launch a dedicated line service incorporating PQC.

South Korea's Ministry of Science and ICT and the National Intelligence Service have established the 'Post-Quantum Cryptography Master Plan' to transition the national cryptographic system to post-quantum cryptography. They have set up a 'National Cryptographic System Transition Task Force' to create an institutional framework for the shift to PQC and will continue to support related technologies and policies.

8.Equal1 and The Irish Centre for High-End Computing Sign Agreement to Advance Quantum Innovation in Ireland and Europe

by Matt Swayne
https://thequantuminsider.com/2024/06/24/equal1-and-the-irish-centre-for-high-end-computing-sign-agreement-to-advance-quantum-innovation-in-ireland-and-europe/?utm_source=newsletter&utm_medium=email&utm_term=2024-06-29&utm_campaign=TQI+Weekly+Newsletter+--+1+000-Plus+Qubits+Centered+on+Excellence+Plus+More+Quantum+News+Industry+Updates

Equal1, one of the world's leading silicon quantum computing companies, has today announced a new cooperation with the Irish Centre for High-End Computing (ICHEC) to advance the deployment of High Performance Computing and Quantum Computing (HPC-QC) in Ireland and Europe to drive technical innovation, address complex scientific and industrial challenges and maintain global competitiveness.

The agreement, in the form of a Memorandum of Understanding (MoU), formalises the mutual interaction and strengthens the existing relationship between Equal1 and ICHEC at the strategic and operational level. Specifically, the organisations together will:

- Promote and position High Performance Computing and Quantum Computing (HPC-QC) in Ireland and Europe as a matter of strategic importance, global competitiveness, and technical research and innovation.
- Engage jointly with other stakeholders to seek national-level funding and support for the operation and services of HPC-QC platforms for enterprise, academic and public sector organisations.
- Leverage national and European programmes to collaboratively develop and engage in R&D on Equal1's quantum computers and subsequent upgrades through 2026.
- Accelerate Quantum-HPC integration by conducting joint RD&I projects towards interoperable coupling and interfacing HPC supercomputers with QC systems.
- Enable Ireland to develop and deploy HPC-QC platforms and services for national users through synergy with the National Strategy for Quantum Technology, EU Quantum initiatives (e.g. Quantum Flagship, EuroHPC JU) and global activities (e.g. IEEE Quantum).

Commenting on the agreement, Venkatesh Kannan, Associate Director at ICHEC said: "ICHEC has a track record since 2018 of strongly positioning Ireland in European and international R&I activities by developing and interfacing HPC and QC technologies in hardware and software infrastructure as well as their use-cases and skills development.

We are excited to formalise this partnership with Equal1. We see huge potential to collaboratively develop the HPC-QC software infrastructure catering to include Equal1's QC technology. This partnership also brings a united front from Ireland for Equal1 and ICHEC to jointly participate in strategic and technology development activities at European and global levels.

The ultimate beneficiaries of the Equal1-ICHEC partnership will be national users across academia, industry and public sector for research, innovation and competence development, propelling the realisation of Ireland's Quantum 2030 National Strategy."

Jason Lynch, CEO of Equal1, commented: "This collaboration marks a significant leap in driving forward innovation and positioning Ireland and Europe at the forefront of the global quantum race. Quantum technology has already shown its potential to materially accelerate growth in areas where Ireland and Europe are currently leaders, surpassing the capabilities of conventional computing.

By working closely with ICHEC, we aim to create a robust ecosystem that integrates High-Performance Computing and Quantum Computing, continuing our journey to make quantum computing accessible

and practical for real-world applications."

9.The 5 Eyes Alliance Can Spy on You Wherever You Are, Here's What You Can Do to Protect Yourself

by Zia Muhammad
https://www.digitalinformationworld.com/2024/06/the-5-eyes-alliance-can-spy-on-you.html

When Edward Snowden revealed that the NSA was secretly spying on American citizens, people began to realize the inherent fragility of the world we are all living in. Snowden's expose shed some light on the murky, interconnected intelligence networks around the world. Most countries have comprehensive intelligence networks, and while they are legally prohibited from spying on their own citizens, collaborations between these agencies provide a bit of a loophole.

Five major nations have banded together to form the Five Eyes alliance. These countries are the US, Canda, the UK, Australia and New Zealand. They share several similarities such as being former British colonies, Anglophone nations as well as having overlapping geopolitical interests with all things having been considered and taken into account.

Another common thread between these nations is that they were all on the same side during World War 2. Hence, it is unsurprising that they decided to join forces in 1946. With the USSR emerging as another superpower to the East, challenging the neoliberal world order that the US and its allies were trying to cement, the Five Eyes alliance attempted to keep the rising red tide at bay.

With all of that having been said and now out of the way, it is important to note that the NSA is the unofficial leader of the Five Eyes alliance. Signatories to the agreement are able to access vast quantities of NSA data, and they return the favor by sharing secret information that they may be in possession of.

The other four countries, namely Australia, New Zealand, Canada and the UK are referred to as second parties. They have the most unrestricted access to NSA data, but it bears mentioning that several other nations have signed on as third parties.

NATO members are all automatically included in the third party list, as are other close US allies such as South Korea. They have more restricted access to the NSA's database, and they also lack other privileges.

Five Eye members are not allowed to spy on each others citizens. This privilege does not extend to third party signatories, thereby running the risk of their confidential secrets falling into the wrong hands. While the general assumption is that Five Eye nations don't spy on each other, there is no way to prove this. After all, the NSA shouldn't have been spying on American citizens either, but this did not stop them from trying to keep tabs on people that had not even committed a crime to begin with.

Apart from the Five Eyes alliance, there are a couple other intelligence networks that include the same five nations along with a few others. First and foremost, the Nine Eyes alliance widens the network to include non-English speaking nations whose goals and interests align with those of the US and its closest allies.

Denmark and Norway joined the **Nine Eyes network** from Scandinavia, with the Netherlands and France also joining from Central and Western Europe. One thing that bears mentioning is that the Nine Eyes alliance is not as official as the Five Eyes alliance. It comprises third party signatories that have certain exclusive privileges, so it is more of an unofficial agreement that does not possess any type of legal backing with all things having been considered and taken into account.

Now, there is another labyrinthine intelligence network that hardly anyone knows about, namely the **14 Eyes Alliance**. One again, the Five Eyes and their formidable intelligence apparatus as at the heart of this alliance, as are the four nations that are included in the nine eyes, but five other major players are thrown into the mix as well.

Each and every one of the members of the additional five are from Europe, including Germany, Sweden, Belgium, Spain and Italy. This clearly shows that the Western powers of the world have extremely close ties, since only North American and European nations are official signatories in any capacity whatsoever.

In spite of the fact that this is the case, a few other nations that go beyond European borders are also seeing an increased level of prominence in global intelligence affairs. We have already mentioned South Korea's inclusion as a third party, with other powerful East Asian nations such as Japan and Singapore also joining it in that regard. Israel is another unofficial member of this exclusive club, with the US frequently propping it up through the provision of military aid.

India and Thailand are also seeing quite a bit of prominence on this front. India is rapidly growing, and it may soon become the largest economy in Asia and perhaps even the entire world. It may be the sole nation that can compete with China for Asian dominance, so Western powers are attempting to bring it into the fold.

China has its own rival intelligence network that it has been building for quite some time now. The rising East Asian great power could potentially end up becoming a superpower on par with the US itself, and it has a range of regional powers that is relying on.

The name of China's alliance is the Shanghai Cooperation Organization. It includes countries in the Russosphere such as Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan as well as Russia itself, along with Pakistan which is notable considering it is a nuclear power. Interestingly, even India is a part of this alliance despite the inclusion of its greatest political rival. This makes India the only nation that is able to toe the line and not pick sides in the global war for domination.

While it might seem like these nations are collaborating in an entirely above board manner, this couldn't be further from the truth. We only know about the informal 14 Eyes Coalition due to a leak, which just goes to show that governments would much prefer to keep these types of things under wraps.

So, what does this mean for the average consumer? Well, for starters, it means that we all need to start being a lot more careful about the manner in which our data is transferred and stored. Given how frequently these nations share data with each other, consumers must be informed about how they can protect themselves.

According to the Electronic Frontier Foundation, these countries can easily bypass what they are referring to as the lowest common privacy denominator. Mass surveillance is at an all time high, and it is up to us to keep ourselves safe from prying eyes.

Many of these countries are trying to codify their attempts at mass surveillance. If any of this legislation ends up getting passed through the requisite legislative bodies, we may end up living in a society where no one would be able to keep a secret from the government.

There are several ways in which we can all keep intrusions at bay. First and foremost, it is imperative that

we start encrypting all of our data. The single best way to go about doing that is by using some kind of a VPN.

A Virtual Private Network sends your data through various digital servers, thereby obscuring your footprint from anyone that may be trying to spy on you. Your internet service provider can monitor your online activities and share it with intelligence agencies if they present a warrant, but with a VPN, they would not have this data to begin with unless they procure it from the VPN provider.

Unfortunately, many VPNs are located in countries that are members of the Five Eyes network. While they might not necessarily give your data up, the countries that participate in this agreement are known for stopping at nothing to get what they need.

A far superior solution would be to use a VPN that is based in a nation that is not a signatory of any intelligence sharing agreements whatsoever. Now, with so many countries freely sharing intelligence, is there really a country out there that can stand out in any capacity?

ProtonVPN might be the answer, since its servers are housed in Switzerland which is famous for being the most privacy friendly country in the world. Switzerland has a long history of being neutral in all conflicts. That can be useful because of the fact that this is the sort of thing that could potentially end up keeping your data completely and utterly safe, no matter how powerful the nation demanding it currently happens to be.

The main benefit of Proton VPN is that it uses something called Perfect Forward Secrecy. This generates an entirely new key for your various browsing sessions, thereby making it so that your other sessions will be perfectly safe even if one of them end up being compromised to any extent whatsoever.

Apart from encrypting your data with a VPN, you should also consider using something similar for your emails. The Five Eyes alliance uses something called **SIGINT** which refers to the interception of transmissions between two points. It was used almost exclusively in warfare, but following the aftermath of the Cold War, it was more and more frequently used to spy on regular everyday citizens.

It stands to reason that your own emails are passing through their filters, but with Proton VPN, these emails will be encrypted. Even if they end up getting intercepted, the information contained within them would not be readable. Only you as well as the intended recipient would be able to read whatever it contains.

Some might also recommend that you use privacy conscious browsers. They don't collect your data similar to Google Chrome and others, thereby giving you an added level of security that you would certainly be grateful for as the global surveillance network becomes ever more powerful.

ProtonVPN yet again offers something quite useful in this regard. Their email service uses a zero trust protocol, which is a level of encryption so advanced that even the company itself would not be able to crack it. On the off chance that an intelligence agency is successfully able to convince Proton Mail to hand over your data, they can simply state that they are unable to do that even if they wanted to.

This allows you to depend on technology rather than an institution and its ethics and morality. No matter how trustworthy a company seems, things like zero trust encryptions can ensure that your privacy will remain unassailable for the foreseeable future.

It would also be extremely useful for you to take a look at messaging apps that offer encryption. Signal and Telegram both stand out, although even something like WhatsApp might get the job done thanks to its end to end encryption.

The global agenda is turning mass surveillance into a foregone conclusion. Even if you don't live in any

of the countries that were mentioned in the Fourteen Eyes Alliance or the Shanghai Cooperation Organization, you might still find yourself under surveillance without any knowledge of what is going on.

The use of ProtonVPN, Proton Mail and other types of services in a similar vein could prove to be the last line of defense. The governments of the world clearly don't care about their citizens, rather they only seem to care about furthering their own ambitions. A decentralized, encrypted future is the only way forward, at least for those that don't want to be under the microscope at all times.

10.India-Based QpiAI Secures $6.5 Million in Pre-Series A Funding

by Matt Swayne
https://thequantuminsider.com/2024/06/21/india-based-qpiai-secures-6-5-million-in-pre-series-a-funding/?utm_source=newsletter&utm_medium=email&utm_term=2024-06-26&utm_campaign=TQI+Weekly+Newsletter+--+Wie+Gehts+IQM+Molecular+Microsoft+Plus+More+Quantum+News+Industry+Updates

QpiAI, a leader in quantum computing and generative AI based in India, has closed its first external investment round, securing $6.5 million in pre-series A funding, according to a story in Outlook India. The round was led by Yournest and SIDBI Venture Capital Limited (SVCL), with participation from a range of other investors.

Participants in the funding round include WFC, an angel group; Ramesh Radhakrishnan, a successful serial entrepreneur and venture capitalist; Ramaswamy Prabhakar, a technologist and angel investor from Silicon Valley; Quick Heal Security founders Kailash Katkar and Sanjay Katkar; Lakshmeenarayanan, former Chairman and CEO of Cognizant; Bhupinder Singh, former CPO of Bentley; Pratap Reddy, a Silicon Valley serial entrepreneur and angel investor; Sahasra Capital, and other angel investors.

With this funding, QpiAI plans to develop a full-stack 25-qubit quantum computer scalable to 1,000 physical superconducting qubits using the same infrastructure. The company also aims to boost revenues from its seven software platforms, including QpiAI-pro, QpiAI-explorer, QpiAI-opt, QpiAI-pharma, QpiAI-ML, QpiAI-logistics, and QpiAI-matter, all of which leverage quantum computing and generative AI technologies.

"Pre-series A round of QpiAI will be remembered as a landmark funding round in Indian deeptech," said Dr. Nagendra Nagaraja, CEO and Founder of QpiAI, as reported in Outlook India . "This round should allow us to lay the foundation of intelligence modeling and intelligence compute via quantum computers and generative AI. Funding will enable us to achieve breakthrough innovation in vertical integration of generative AI and quantum computing in enterprise and industrial applications."

QpiAI, already a revenue-generating enterprise-focused technology startup, counts Fortune 500 companies in pharmaceuticals, materials, chemicals, cosmetics, automotive, financials and manufacturing among its customers, according to the news magazine.

As part of the funding agreement, Debraj Banerjee from SIDBI Ventures will join the QpiAI board as a nominee of SIDBI Venture Capital. Ramesh Radhakrishnan, the first external investor in QpiAI, will join the board as a nominee director of Qpi Technology, the holding company of QpiAI.

"Building scalable quantum computers that can solve real-world problems and bolster our industry verti-

cals is a key technology development," said Dr. Manjunath R.V., Vice President for Quantum Computers at QpiAI. "At QpiAI, we are very excited to have our own quantum computers to further build quantum and AI data centers. Our team is thrilled to advance our roadmap to scale quantum computers from 25 qubits to 1,000 qubits."

The funding will also support the development of 25-qubit quantum computers at QpiAI's Bangalore headquarters by Q4 2024 or Q1 2025. The integration of high-performance computing (HPC) with quantum capabilities will help pave the way for innovation in QpiAI's generative AI and quantum software products. The company plans to offer Quantum Compute as a Service (QCaaS) and provide comprehensive Quantum-HPC solutions to its customers.

"By investing in QpiAI, we're helping to propel India to the leading edge of quantum computing," said Sunil Goyal, MD of Yournest. "This technology has the potential to revolutionize fields like materials science, drug discovery, automotive, and manufacturing. QpiAI's innovative approach makes them a key player in unlocking this potential, and we're thrilled to join Dr. Nagendra and the QpiAI team on this exciting journey."

Sachin Kumar, Lakshya Priyadarshi, and Aswanth Krishnan, who lead QpiAI's software products and solutions in generative AI and quantum software, noted, "In the last four years, we were able to commercialize our software platforms and achieve traction across large blue-chip enterprise customers. With this funding, and with all our seven software products ready to scale, we envision scaling our software platforms globally."

QpiAI, headquartered in Bangalore, India, with subsidiaries in the US and Finland, plans to expand its presence in global markets, including the US, Europe, Japan, the Middle East, and Southeast Asia.

"Quantum computers and AI are the future for all applied technologies in many different market segments," said Ramesh Radhakrishnan. "Integrating application software with quantum system software and hardware to make AI and quantum computing work together is a fundamental innovation whose significance is going to be enormous."

11.Innovation vs. imitation: The cryptographic signature evolution

by Padmakumar Nair
https://www.expresscomputer.in/guest-blogs/innovation-vs-imitation-the-cryptographic-signature-evolution/113180/

In a world where technological developments drive economic progress and security, the distinction between innovation and imitation has never been more important. Markets worldwide are plagued by counterfeit products, ranging from luxury handbags to crucial aircraft components. Cryptographic signatures, unknown to many in the field of digital security, are altering industries by ensuring data authenticity, integrity, and non-repudiation.

However, as technology progresses, the issue of discerning real innovation from imitation grows, as does the question of why cryptographic signatures embody this paradox, influencing the future of secure communications and transactions.

Counterfeit goods represent a significant global problem, affecting industries from fashion to pharma-

ceuticals. According to a joint report by Crisil and the Authentication Solution Providers Association (ASPA), around 25–30% of all products marketed in the nation are fake. The most prominent product categories where customers encounter counterfeit goods are clothing (31%), FMCG (28%), and automobiles (25%), with pharmaceuticals (20%), consumer durables (17%), and agrochemicals (16%) following closely afterwards. The World Health Organization (WHO) reports that poor-quality and counterfeit pharmaceuticals affect 10.5% of low- and middle-income countries (LMICs) and cost an estimated $30.5 billion annually.

Potential of cryptographic signatures

Cryptographic signatures are an essential component of modern security systems, allowing users to verify the origin and integrity of digital messages and documents. Cryptographic signatures use a pair of keys—a private key for establishing the signature and a public key for verification—to ensure that any changes to the data after signing are traceable. This technique is critical for a variety of applications, including email security and blockchain transaction validation. Traditional anti-counterfeiting measures, such as holograms, barcodes, and RFID tags, have been in place for years, but counterfeiters continuously evolve their methods to bypass these defenses. In this ongoing cat-and-mouse game, the need for more robust and innovative solutions is clear.

Invisible signatures represent an innovative evolution in the realm of cryptographic signatures, offering enhanced security and versatility in combating counterfeiting and fraud. Unlike traditional signatures, which may be visible and susceptible to replication or tampering, invisible signatures are embedded within the digital fabric of documents or products, making them virtually undetectable to the naked eye. The technology behind invisible signatures typically involves advanced cryptographic techniques, such as steganography or digital watermarking, to hide the signature within the content itself. This hidden signature can encode critical information about the document or product, including its origin, authenticity, and ownership, without altering its visual appearance or usability.

The potential benefits of invisible signatures for society are multifaceted:

- **Enhanced security:** Invisible signatures provide an additional layer of security against counterfeiting and fraud by creating unique identifiers that are difficult to replicate or alter. This helps protect consumers, businesses, and governments from the economic and reputational damages associated with counterfeit goods or forged documents.
- **Traceability and accountability:** By embedding invisible signatures in digital assets, such as electronic documents or digital media, it becomes possible to trace their origin and ownership throughout their lifecycle. This facilitates accountability and enables better enforcement of intellectual property rights, copyright protection, and supply chain integrity.
- **Streamlined authentication:** Invisible signatures streamline the authentication process for digital transactions, communications, and interactions. Users can verify the authenticity and integrity of documents or products quickly and reliably, without the need for specialized equipment or expertise.
- I**ntegration with emerging technologies**: Invisible signatures are compatible with emerging technologies, such as blockchain and Internet of Things (IoT) devices, enabling seamless integration into decentralized networks and smart systems. This opens up new possibilities for secure and transparent value exchange, automated verification, and data-driven insights.
- **Sustainable solutions:** Unlike physical anti-counterfeiting measures, such as holograms or RFID tags, invisible signatures are inherently digital and do not require additional materials or resources for implementation. This makes them a more sustainable and environmentally friendly solution for combating counterfeiting and protecting intellectual property.

Overall, invisible signatures represent a promising advancement in the field of anti-counterfeiting, offering a potent tool for safeguarding digital assets and cultivating trust in the digital economy. As technolo-

gy continues to evolve, invisible signatures are poised to play a crucial role in ensuring the integrity, authenticity, and security of digital interactions across various sectors and industries.

Innovation: Cultivating new frontiers

The essential heart of cryptographic signature innovation is the creation of new algorithms and protocols to improve security, efficiency, and scalability. Innovations such as quantum- resistant algorithms are being investigated in order to future-proof cryptographic systems against the possible threat posed by quantum computing. Similarly, advances in multi- signature schemes provide more flexible and secure digital asset management, which is critical for DeFi applications and beyond.

Furthermore, the integration of cryptographic signatures with future technologies such as the Internet of Things (IoT) and artificial intelligence (AI) is creating new opportunities. For example, secure IoT ecosystems use cryptographic signatures to verify that data exchanged between devices is genuine and untampered, which addresses a crucial concern in the age of connected gadgets.

Balancing innovation and imitation in cryptographic practices

While innovation propels progress, imitation aids in standardising and spreading proven technologies. Nonetheless, excessive dependence on imitation can hinder advancement and expose systems to new threats.

Standardisation vs. stagnation: Interoperability and widespread acceptance are guaranteed by the use of standardized cryptographic methods. Adoption of new, more secure techniques, however, can be hampered by an overemphasis on current standards. It is critical to strike a balance between adopting cutting-edge technologies and utilizing tried-and-true methods.

Interoperability and acceptance are ensured by standardized brand protection methods, but overemphasis on current standards can hinder the adoption of new techniques. For example, relying on traditional trademark registration systems over innovative approaches like invisible signatures can expose brands to counterfeiting. Traditional systems are often lengthy and may not address modern digital threats. In contrast, invisible signatures,
embedded using microtext, UV inks, or digital watermarks, provide a secure method for verifying product authenticity. These are difficult to replicate and can be quickly verified with specialized tools. Embracing such innovations enhances brand protection and trust, balancing traditional methods with modern security needs.

Security risks: Products may be left vulnerable if outdated anti-counterfeit techniques are imitated without considering new counterfeiting tactics. The methods employed to prevent counterfeiting must also evolve over time. Relying on antiquated techniques can lead to serious security breaches and the proliferation of counterfeit goods.

Cost and complexity: Putting new cryptographic solutions into practice can be perceived to be expensive and complicated, which is why some businesses choose to opt for more streamlined, well-known techniques. As a result of future security breaches and required updates, this may save initial costs and complexity but increase long-term risks and expenses.

Bridging the balance

The balance between originality and imitation is tricky yet critical. True innovation in cryptographic signatures necessitates a dedication to advancing the technology, predicting future obstacles, and always upgrading security measures. This entails not only technical innovation but also cultivating a culture of forward-thinking and resilience to complacency.

Organisations and developers must prioritize rigorous testing, peer review, and adherence to industry standards to guarantee that new cryptographic signature implementations are both innovative and secure. This allows them to avoid the dangers of imitation while still contributing to the solid security infrastructure required for the digital age. Raising awareness about the dangers of counterfeit products and promoting the adoption of advanced manufacturing technologies can help build a more informed and resilient market. Encouraging consumers to verify the authenticity of products and report suspected counterfeits can further strengthen these efforts.

Cryptographic signatures are designed to ensure authenticity and prevent imitation, highlighting the importance of continual innovation to stay ahead of counterfeiters. As the digital landscape evolves, engineers, legislators, and industry leaders must encourage true innovation while being cautious against challenges posed by imitation. Only by taking such a balanced approach can we fully realize the potential of cryptographic signatures to protect
our digital future. Imagine a world where every buyer is vigilant about quality and every product's authenticity is ensured through cutting-edge technology. With the right strategies and technologies in place, we can tip the scales in favor of innovation and ensure a safer, more authentic marketplace.

12.Why Quantum Random Numbers are key to safety against Quantum Computers

by Jose Coello
https://cryptalabs.com/why-quantum-random-numbers-are-key-to-safety-against-quantum-computers/

Quantum computing poses a significant threat to the current Public Key Infrastructure (PKI) through Shor's Algorithm, which can efficiently factorize large numbers, potentially breaking widely used encryption schemes. Additionally, Grover's Algorithm presents a lesser-known but equally critical threat by enabling a quadratic speedup in searching unstructured databases, which can undermine the security of random number generation reliant on entropy expansion.

Quantum Mechanics and Random Number Generation

Quantum mechanics, the first scientific description of nature that is not fully deterministic, allows us to harness phenomena like the Heisenberg Uncertainty Principle and quantum superposition to generate truly unpredictable random numbers. Quantum Random Number Generators (QRNGs) leverage these principles to produce randomness several orders of magnitude faster than current classical Random Number Generators (RNGs).

Current Limitations of Classical RNGs

Classical RNGs are relatively slow, operating at speeds around hundreds of Kbit/s. To address this bottleneck, methods to expand entropy, such as using hash functions like SHA2-256, have been developed. This process involves inputting a seed from the random number source and using a counter to expand it, generating pseudo-random numbers by incrementing the counter while keeping the seed constant. However, this approach is vulnerable to attacks using Grover's Algorithm, which can reduce the security of a 256-bit implementation to the equivalent of 128-bit security under attack. Advances in hybrid quantum/classical algorithms further weaken the security of hash functions, potentially reducing their effective security below 128 bits.

Advantages of QRNGs

QRNGs can circumvent the problem of entropy expansion attacks by providing high-speed, truly unpredictable randomness without the need for expansion. For example, Crypta Labs QRNGs can reach speeds of Mbit/s and Gbit/s, significantly enhancing cybersecurity frameworks by supporting the 'Zero Trust' model in critical infrastructure.

The Urgent Need for Quantum-Safe Cryptography

The transition to quantum-safe cryptography is imperative. To achieve this, it's essential not only to implement post-quantum algorithms approved by NIST but also to use QRNGs that avoid entropy expansion. There are two primary solutions for mitigating the threat of quantum computers: post-quantum algorithms (PQ) and quantum key distribution (QKD). Each has its pros and cons, but QRNGs are crucial in ensuring both computational and mathematical security in QKD. While PQ algorithms focus on resisting Shor's Algorithm, they also require robust entropy sources, making the integration of QRNGs vital for secure implementation.

In conclusion, to effectively protect against the evolving threats posed by quantum computing, integrating QRNGs into cybersecurity measures is essential. This integration ensures the generation of truly unpredictable random numbers, thereby bolstering the security of both PQ algorithms and QKD systems.

13.PQShield raises funding for commercial adoption of quantum resistant cryptography

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/pqshield-raises-funding-for-commercial-adoption-of-quantum-resistant-cryptography/

PQShield, a cybersecurity company specializing in post-quantum cryptography (PQC), has raised $37 million in Series B funding led by Addition, with participation from new investors Chevron Technology Ventures, Legal & General and Braavos Capital, together with existing backers, Oxford Science Enterprises.

PQShield will use the funding to expand its commercial operations as it continues to meet growing global demand for its quantum-ready cryptography offerings for hardware, software and communications, as well as its research IP.

The National Institute of Standards & Technology's (NIST) post-quantum cryptography standards are due to be ratified in a matter of weeks, marking an inflection point in the global transition to quantum security. NIST's standards are also likely to be adopted by the International Organization for Standardisation (ISO). With new global standards in place and a series of government directives, such as the US National Security guidance (e.g., CNSA 2.0), mandating the migration of critical systems to PQC from 2025, it's now a commercial imperative to adopt PQC. This is particularly so where an organization has critical data it needs to keep secure for any length of time — in fact, if they haven't already started planning the transition, they are already behind.

Since it was founded in 2018, PQShield has established an industry-leading team of cryptography and engineering experts who have built an extensive, secure product suite for use in hardware, software, and the cloud. Recent strategic US hires include Johannes Lintzen, who joins from Cryptomathic as Global Business Development Director, and Janssen Liston, who joins from Rambus as North America Senior Sales Director.

PQShield's cryptographic products are already helping to facilitate the transition to quantum security throughout the global technology supply chain — for example, in the secure boot and update of devices, in the Hardware Security Modules (HSMs) that secure most financial transactions, in ever-more connected vehicles, and in military grade communications systems.

As well as advising businesses on the transition to quantum security, the company plans to also continue to support governments, industry bodies and cybersecurity agencies as they develop guidance around the migration to PQC. PQShield continues to play a leading role in the NIST PQC standardization project (having co-authored all four announced standards), and will continue to advise the White House, European Parliament, UK National Cyber Security Council (NCSC) and World Economic Forum (WEF) on the practical challenges involved.

Todd Arfman of Addition said: "As we approach the culmination of the NIST project, we expect newly-ratified standards to help drive rapid adoption of PQC across the technology supply chain. Led by an industry-leading team with decades of experience, PQShield has quickly established itself as a leading authority in post-quantum cryptography for hardware and software. We are excited to see the business continue to build on its existing commercial success and further enhance its efforts in protecting our digital future."

PQShield CEO and founder, Ali El Kaafarani, said: "It no longer matters when a quantum computer will arrive that can break current cryptography methods: the need for quantum-resistant encryption is here today, as governments and standards agencies push to protect our most sensitive data."

"We're already getting our technology into the hands of customers across the supply chain, and today's funding will enable us to deliver real-world, post-quantum hardware and software upgrades to even more organizations as they move to comply with new global standards."

"It's our responsibility to deliver security and privacy in an increasingly digital world. Every line of code we write, every mathematical problem we solve, and every interaction we make is focused on one specific goal: keeping us all one step ahead of the attackers."

14.Crypto-agility and quantum-safe readiness

by Ray Harishankar, Michael Osborne, Jai S. Arun, John Buselli, and Jennifer Janechek
https://www.ibm.com/quantum/blog/crypto-agility

With the US National Institute of Standards and Technology (NIST) post-quantum cryptographic standard expected to be published this summer, companies need to start navigating the migration to quantum-safe cryptography. The most sustainable and effective way to make cryptosystems resilient for the quantum era is to establish cryptographic agility, or crypto-agility for short.

Crypto-agility means that a system, platform, application, or organization can rapidly adapt its crypto-

graphic mechanisms and algorithms in response to changing threats, technological advances, or vulnerabilities. However, what crypto-agility looks like in practice is less obvious. Crypto-agility is not just about transitioning to quantum-safe cryptography in the nimblest way possible, and it's not something that can be achieved merely by updating encryption algorithms and protocols. Instead, you need to adapt your organization's cryptographic architecture, automation, and governance to allow for greater control and flexibility as you work to anticipate evolving cyber threats efficiently and with minimal disruption.

Why is crypto-agility important?

New quantum-safe cryptography standards will continue to emerge along with new regulations for security protocols as quantum computing technology advances. Therefore, you must be able to quickly locate and update cryptography across your IT landscape to address emerging cyber threats and vulnerabilities. That means understanding where cryptography is deployed across all the dependent components in a system and how it is implemented in each component. For example, a Java application containing sensitive client data may be built using the Java language, but it will contain many third-party dependencies that contain cryptography, such as a Java framework, a Java virtual machine, a database component, remote APIs, the operating system, and the hardware on which it is deployed. Each of these components may integrate cryptography differently, making it important to understand cryptography usage in the context of system dependencies.

Crypto-agility also manifests at the level of algorithm design and assurance. Cryptography providers should ensure that there are different algorithm implementations for different security strengths and that the algorithms dynamically scale in security strength based on configuration. But most problems result from flaws in the algorithm implementations themselves. For example, block ciphers are susceptible to implementation flaws through the improper use of their mode of operation, or the algorithm that cryptographically transforms the data based on the block cipher. Implementation flaws can also result from misusing cryptographic primitives, such as by improperly combining them in protocols. Therefore, you need to maintain ongoing visibility into your cryptographic ecosystem so that you can identify potential cryptographic weaknesses and remediate them quickly.

The principles of crypto-agility can give you greater control over the configuration and deployment of cryptography by abstracting and simplifying the way you interact with it. Rather than settling for cryptographic components that use low-level cryptographic APIs, you can work toward using application interfaces, design patterns, microservices, and policy configuration frameworks that facilitate migration across implementations. These interfaces should also properly handle the challenge of programming language bindings — libraries that serve as a bridge between different programming languages to enable a library to be used for a different language than the one it was written for.

Lastly, crypto-agility drives alignment between stakeholders within the enterprise and across the cryptography life cycle. Cryptography researchers, providers, and consumers can work together to create more responsive cybersecurity architectures through a shared focus on creating structures that make cryptography implementations flexible and scalable. As an added benefit, this reduces the chances that cryptographic libraries and algorithms will be misused.

Building crypto-agility might seem like a significant undertaking, but the quantum-safe migration is the perfect time to begin this work. Regardless of your organization's current level of security maturity, you can use a framework centered on architecture, automation, and governance to establish crypto-agility in and beyond your transition to quantum-safe cryptography.

Crypto-agility requires modularity and abstraction

When NIST announced its program to solicit, evaluate, and standardize post-quantum cryptographic

algorithms in 2016, it prompted organizations to begin considering what quantum-vulnerable cryptography they might be using.

These efforts revealed that locating cryptography within business applications is like searching for a "needle in a haystack," and tracking it down across the supply chain can prove even more difficult. If you can identify it in third-party components, you rely on the provider to make the necessary changes.

Cryptographic discovery can require a lot of time and resources. A more agile cryptographic infrastructure would simplify this process in the future by centralizing and abstracting cryptography so that you can monitor and update it without digging into application code. This entails decoupling cryptography from applications, instead driving configuration from middleware, sidecars, and/or platforms. An agile cryptographic architecture also employs modularity through abstraction layers, isolating the applications, systems, and network from specific cryptographic implementations. This, in turn, allows systems to support multiple encryption algorithms and providers interchangeably. For their part, cryptography providers can promote crypto-agility by transitioning from cryptographic libraries to services, engines, and sidecars.

Crypto-agility requires automation

A crypto-agile framework also means using automation to dynamically manage cryptographic parameters, encryption, keys, and certificates across the IT landscape. Automation tools and scripts can handle tasks like key generation, rotation, and updating cryptographic settings based on predefined policies or events. This helps organizations develop operational agility as they adapt cryptographic implementations to accommodate changing security requirements.

Moreover, managing cryptography within a framework of crypto-agility entails centralizing the routine collection of cryptographic metadata and usage logs. Automating these processes enables you to detect potential vulnerabilities in real time and maintain continuous compliance.

Crypto-agility requires governance

Cryptographic governance is just as critical to crypto-agility as building more efficient configuration and management processes. Governance requires the ability to understand where and how cryptography is used, as well as the ability to initiate and monitor changes. Most of the cryptography that organizations use is in third-party components and applications, making it essential to include the supply chain in the governance scope. Standards such as the Cryptography Bill of Materials (CBOM), now included in the CycloneDX 1.6 standard and supported by IBM Quantum Safe Explorer, can be used to help understand and govern the supply chain.

Within every organization, CISOs, security architects, DevSecOps engineers, application developers, and other stakeholders should align on the definition and enforcement of policies related to cryptographic algorithms and practices. This team should work together to create a system for adhering to industry standards, selecting appropriate cryptographic algorithms based on security needs, ensuring compliance with regulatory requirements, and updating or retiring outdated cryptography. Much of this work can be centralized in a Cryptographic Center of Excellence (CCoE), where a cross-functional team collaborates to promote awareness and training in the latest standards, review proposed cryptographic architectures, and develop policies that support agile design patterns and dynamic cryptography management. An internal CCoE can then align with industry- and association-backed centers of excellence, such as the NIST Cybersecurity Center of Excellence (NCCoE), to explore the latest guidance on and use cases for cryptographic implementations and remediation patterns.

How IBM Quantum Safe can help you build crypto-agility

To help you establish crypto-agility throughout your quantum-safe journey, we developed IBM Quantum Safe technologies that build simplicity, flexibility, and automation into your quantum-safe transformation roadmap.

With our discovery and observability tools, you can locate cryptographic artifacts in data at rest and data in transit. IBM Quantum Safe Explorer identifies cryptography across portfolios of applications, analyzes dependencies, and creates a cryptographic inventory. Our quantum-safe cryptographic posture management tool further supports operational agility. By automating metadata aggregation across the entire enterprise IT landscape and providing policy-based vulnerability identification that integrates with your ticketing system, you can monitor and strengthen your cryptographic posture as your modernize your broader cybersecurity infrastructure. This, in turn, supports a more robust governance model that enables stakeholders to monitor compliance, track remediation progress, and make better informed policy decisions.

As of May, organizations can take a major step toward building a more agile cryptographic architecture using the adaptive proxy utility offered through IBM Quantum Safe Remediator. This network remediation tool enables you to position an intermediary between all client types and your business applications. The tool supports classical, quantum-safe, and hybrid forms of cryptography, allowing you to migrate heterogeneous infrastructures in a step-by-step and agile fashion that minimizes business disruption. The adaptive proxy also collects metrics so that you can track your organization's progress along the quantum-safe journey. Additionally, IBM Quantum Safe Remediator provides a performance test harness utility that enables you to test various combinations of quantum-safe cryptographic algorithms. Using this capability, organizations can understand the impact of different post-quantum algorithm combinations on their infrastructure and select the best migration approach.

IBM Quantum Safe fosters agility throughout every step of the migration to quantum-safe cryptography. Whether you are just beginning the cryptographic discovery process or are already well into the transition to post-quantum cryptography, we will support you with the tools, approaches, and strategies you need to create your quantum-safe future. Start building crypto-agility today by identifying and inventorying your cryptographic assets, establishing a governance model to monitor and strengthen your cryptographic risk posture, and incrementally transitioning to quantum-safe cryptography while building a stronger, smarter cybersecurity framework for the quantum era.

15.Authenticating in a Post-Quantum World

by James Dargan
https://thequantuminsider.com/2024/06/19/authenticating-in-a-post-quantum-world/

At the first Future Cryptography Conference held in Tallinn, Estonia, the primary focus was on Post-Quantum Cryptography (PQC). With the advent of quantum computing, traditional cryptographic methods face obsolescence, necessitating a new paradigm in secure communication. Esteemed experts from Estonia and Czechia gathered to deliberate on the challenges and advancements in PQC, addressing standards, applications, and strategies for migration to these new technologies.

One of the most compelling presentations was by Peeter Laud, a Senior Researcher at Cybernetica, who tackled the intricate question: *"How will I authenticate myself in a post-quantum world?"* His presentation went deep into the core of authentication in a future dominated by quantum computing.

Laud's discussion began with the fundamental need for authentication — ensuring secure connections and safeguarding cryptographic material. He posed crucial questions about identity: What constitutes "me"? Is it just a name, date of birth, personal code, biometrics, or a combination of these? In the realm of cryptographic protocols, it involves public keys bound to individuals by certificates, which are then signed by trusted authorities. The use of private keys for cryptographic operations is essential in this context.

Laud paid attention to the disparity in the capability of current devices to execute PQ crypto algorithms and protect cryptographic material. Devices such as computers, smartphones, secure elements, embedded devices, and smart cards each have varying levels of support for PQ authentication protocols. For relying parties, computers (servers) and Hardware Security Modules (HSM) are pivotal as they need to compute digital signatures.

Laud stressed the potential of threshold cryptography in post-quantum authentication. However, existing threshold protocols for algorithms like Dilithium are currently too inefficient for practical applications like Smart-ID. Yet, these protocols are "generic," and optimizing them for specific settings, such as two-party scenarios, could overcome inefficiencies. Laud introduced TOPCOAT, a Dilithium-inspired threshold signature scheme designed for two signing parties, showcasing its practical efficiency while relying on lattice-based hardness assumptions.

The presentation also touched on the theoretical underpinnings of quantum security. Laud discussed the quantum reductions and how some hardness assumptions hold even in the presence of quantum adversaries. Although many cryptographic constructions, including TOPCOAT, only have classical proofs of security, there is ongoing research to establish quantum reductions.

Looking ahead, Laud outlined a way forward involving secure multiparty computation (SMC) protocols and the role of correlated randomness. Practical deployment of these protocols requires considerations of performance and the isolation between server and correlated randomness generators.

This discussion at the Future Cryptography Conference is part of a broader conversation, including Estonia's roadmap for encryption in the age of quantum computing. As detailed in the earlier piece: *Estonia's Roadmap For Encryption In The Age Of Quantum Computing* *The Quantum Insider* published from the same conference, Estonia is taking proactive steps in preparing for a post-quantum world, ensuring that its cryptographic infrastructure remains robust and secure.

Laud's insights underscore the complexity and necessity of evolving our authentication methods to meet the challenges posed by quantum computing. As research and development continue, the integration of these advanced cryptographic techniques will be crucial in safeguarding our digital identities in the quantum era.

16.Smart Guessing Algorithm Cracks 87 Million Passwords in Under 60 Seconds

by Davey Winder
https://www.forbes.com/sites/daveywinder/2024/06/19/smart-guessing-algorithm-cracks-87-million-passwords-in-under-60-seconds/

With just a few dollars, a little time, and a smart brute-force guessing algorithm, most passwords can be cracked in much less time than you might imagine. According to a new analysis from the experts at

Kaspersky, 59% of 193 million actual passwords were cracked in less than 60 minutes, and 45% were cracked in less than 60 seconds.

The basis of a brute-force attack is where the perpetrator iterates all possible combinations in order to find a match for the password in question. However, Antonov explained, “smart guessing algorithms are trained on a passwords data-set to calculate the frequency of various character combinations and make selections first from the most common combinations and down to the rarest ones.”

Brute Force And Smart-Guessing Combine To Quickly Crack Passwords

Although very popular due to the point-and-fire simplicity of a brute-force attack, it remains suboptimal as far as password-cracking algorithms are concerned. When you consider that the vast majority of passwords in daily use contain similar characteristics involving the combination of dates, names, dictionary words and keyboard sequences, adding these to the guessing-game mix speeds things up considerably.

The Kaspersky study revealed that when it comes to the percentage of passwords crackable in any timeframe using each method, while 10% of the password list analyzed was broken in under a minute by brute force, that increased to 45% when smart-guessing was added to the algorithm. Allowing for between a minute and an hour, the difference was 20% compared to 59%.

The Smart-Guessing Algorithm Advantage Explained

Because humans are creatures of habit, we make for very poor password creators. The truth is that the passwords we choose for ourselves are rarely, if ever, truly random. We rely upon all the things that smart-guessing algorithms are designed to detect: common names and phrases, important dates both personal and historical, and patterns, lots of patterns. To give you an idea of how predictable we are, one YouTube channel took a sample of more than 200,000 people and asked them to choose a ‘random’ number between 1 and 100. Most people gravitated towards the same relatively small set: 7, 37, 42, 69, 73, and 77. Even when trying to be random with character strings, we fail as most people will favor the center of the keyboard for their selection, according to Kaspersky.

“Smart algorithms make short work of most passwords that contain dictionary sequences,” Antonov said, “and they even catch character substitutions.” In other words, using p@ssw0rd instead of password won’t slow the algorithm down that much at all.

How To Strengthen Your Accounts Against Smart-Guessing Algorithm Attack

Kaspersky recommends the following password usage strategy:

- Generate strong and truly random passwords using a password manager.
- Don’t reuse passwords across sites and services or hacking one basket will enable access to many more eggs.
- If you don’t, or won’t, use a password manager, then use mnemonic passphrases rather than dictionary words and numeric combinations.
- Don’t save passwords in web browsers.
- Use a password manager protected by a strong master password.
- Use two-factor authentication for all accounts that support it.

17.Post-Quantum Cryptography Success Relies on a Strong Workforce

by Silvia Oakland
https://govciomedia.com/post-quantum-cryptography-success-relies-on-a-strong-workforce/

Federal cybersecurity leaders are calling for the federal workforce to increase understanding of post-quantum cryptography and protecting data as adversaries like China build up their investments in the technology.

“If you are working on quantum and you’re not including your cyber team, you’re doing everyone a disservice,” said Amy Hamilton, visiting faculty chair from the Department of Energy at National Defense University, at ATARC’s inaugural Federal Quantum Summit last month. “The really important thing is that we’re all at the table talking because all of these new technologies are going to enable and empower our lives in ways that we can’t imagine.”

Currently, the cybersecurity workforce understands classical-quantum algorithms, but it isn’t as familiar with post-quantum cryptography algorithms. There is urgency to change that reality as adversaries like quantum pour investments into it, Hamilton added.

“These algorithms are nothing like we’ve ever used before, in many respects. It’s going to change the paradigm of how we approach and look at cybersecurity in general,” noted IBM Quantum-Safe Executive Robert Campbell. “They should not be separated; you can’t have cybersecurity without quantum cryptography.”

Campbell said the technology, along with zero trust and AI, all needs to be a part of classroom discussions starting in high school. Beginning these conversations earlier can allow for a better understanding of how they work in tandem rather than waiting to explain the concepts when students enter the workforce.

Likewise for the military, said Marine Corps Cyberspace Command Cyber Technology Officer Shery Thomas.

“You’ve probably heard, ‘Every Marine is a rifleman.’ We’re going to modify that,” Thomas said. “Every Marine is also a technologist and integrator, too, because every single thing they touch, whether it be that small screen or something on an aircraft, they’re touching technology.”

The transition to post-quantum cryptography for all agencies will be a long process, according to Cybersecurity and Infrastructure Security Agency (CISA) Senior Engineer and ICAM Subject Matter Expert Ross Foard. CISA is helping agencies understand, prepare and make changes to the algorithms through a roadmap that will be released later this summer.

“It’s really important to discover where these functions are in use today and then to make an inventory of all those things it’s protecting,” Foard said. “Knowing the inventory of what those functions are protecting is really important.”

“We just implemented our USDA data strategy plan in December for the next five years. In conjunction with that, they’re working to develop more of a posture for cybersecurity in post-quantum cryptography,”

added Agriculture Department IT Manager Rudolph Rojas.

Although there are still many unknowns about what quantum computing can offer, but researchers see opportunity.

“The reality is, we still don’t know what quantum technology can offer to humanity in terms of quantum computing,” said Davide Venturelli, associate director of quantum technologies at the Universities Space Research Association. “There’s a lot of more questions to be asked, then there are solutions to be implemented right now.”

18.Themes from Real World Crypto 2024

https://blog.trailofbits.com/2024/06/18/themes-from-real-world-crypto-2024/

In March, Trail of Bits engineers traveled to the vibrant (and only slightly chilly) city of Toronto to attend Real World Crypto 2024, a three-day event that hosted hundreds of brilliant minds in the field of cryptography. We also attended three associated events: the Real World Post-Quantum Cryptography (RWPQC) workshop, the Fully Homomorphic Encryption (FHE) workshop, and the Open Source Cryptography Workshop (OSCW). Reflecting on the talks and expert discussions held at the event, we identified some themes that stood out:

1. Governments, standardization bodies, and industry are making substantial progress in advancing post-quantum cryptography (PQC) standardization and adoption.

2. Going beyond the PQC standards, we saw innovations for more advanced PQC using lattice-based constructions.

3. Investment in end-to-end encryption (E2EE) and key transparency is gaining momentum across multiple organizations.

We also have a few honorable mentions:

1. Fully homomorphic encryption (FHE) is an active area of research and is becoming more and more practical.

2. Authenticated encryption schemes with associated data (AEADs) schemes are also an active area of research, with many refinements being made.

Read on for our full thoughts!

How industry and government are adopting PQC

The community is preparing for the largest cryptographic migration since the (ongoing) effort to replace RSA and DSA with elliptic curve cryptography began 25 years ago. Discussions at both the PQ-dedicated RWPQC workshop and the main RWC event focused on standardization efforts and large-scale real-world deployments. Google, Amazon, and Meta reported initial success in internal deployments.

Core takeaways from the talks include:

- The global community has broadly accepted the NIST post-quantum algorithms as standards. Higher-level protocols, like Signal, are busy incorporating the new algorithms.

- Store-now-decrypt-later attacks require moving to post-quantum key exchange protocols as soon as possible. Post-quantum authentication (signature schemes) are less urgent for applications following good key rotation practices.
- Post-quantum security is just one aspect of cryptographic agility. Good cryptographic inventory and key rotation practices make PQ migration much smoother.

RWPQC featured talks from four standards bodies. These talks showed that efforts to adopt PQC are well underway. Dustin Moody (NIST) emphasized that the US government and US industries aim to be quantum-ready by 2035, while Matthew Campagna (ETSI) discussed coordination efforts among 850+ organizations in more than 60 countries. Stephanie Reinhardt (BSI) warned that cryptographically relevant quantum computers could come online at the beginning of the 2030s and shared BSI's Technical Guideline on Cryptographic Mechanisms. Reinhardt also cautioned against reliance on quantum key distribution, citing almost 200 published attacks on QKD implementations. NCSC promoted the standalone use of ML-KEM and ML-DSA, in contrast to the more common and cautious hybrid approach.

While all standards bodies support the FIPS algorithms, BSI additionally supports using NIST contest finalists FrodoKEM and McEliece.

Deidre Connelly, representing several working groups in the IETF, talked about the KEM combiners guidance document she's been working on and the ongoing discussions around KEM binding properties (from the CFRG working group). She also mentioned the progress of the TLS working group: PQC will be in TLS v1.3 only, and the main focus is on getting the various key agreement specifications right. The LAMPS working group is working on getting PQC algorithms in the Cryptographic Message Syntax and the Internet X.509 PKI. Finally, PQUIP is working on the operational and engineering side of getting PQC in more protocols, and the MLS working group is working on getting PQC in MLS.

The industry perspective was equally insightful, with representatives from major technology companies sharing some key insights:

Signal: Rolfe Schmidt gave a behind-the-scenes look at Signal's efforts to incorporate post-quantum cryptography, such as their recent work on developing their post-quantum key agreement protocol, PQXDH. Their focus areas moving forward include providing forward-secrecy and post-compromise security against quantum attackers, achieving a fully post-quantum secure Signal protocol, and anonymous credentials.

- **Meta/Facebook:** Meta demonstrated their commitment to PQC by announcing they are joining the PQC alliance. Their representative, Rafael Misoczki, also discussed the prerequisites for a successful PQC migration: cryptography libraries and applications must support easy use of PQ algorithms, clearly discourage creation of new quantum-insecure keys, and provide protection against known quantum attacks. Moreover, the migration has to be performant and cost-efficient.

- **Google:** Sophie Schmieg from Google elucidated their approach toward managing key rotations and crypto agility, stressing that post-quantum migration is really a key rotation problem. If you have a good mechanism for key rotation, and you are properly specifying keys as both the cryptographic configuration and raw key bytes rather than just the raw bytes, you're most of the way to migrating to post-quantum.

- **Amazon/Amazon Web Services (AWS):** Matthew Campagna rounded up the industry updates with a presentation on the progress that AWS (AWS) has made towards securing their cryptography against a quantum adversary. Like most others, their primary concern, is "store now, decrypt later" attacks.

Even more PQC: Advanced lattice techniques

In addition to governments and industry groups both committing to adopting the latest PQC NIST standards, RWC this year also demonstrated the large body of work being done in other areas of PQC. In particular, we attended two interesting talks about new cryptographic primitives built using lattices:

- **LaZer:** LaZer is an intriguing library that uses lattices to facilitate efficient Zero-Knowledge Proofs (ZKPs). For some metrics, this proof system achieves better performance than some of the current state-of-the-art proof systems. However, since LaZer uses lattices, its arithmetization is completely different from existing R1CS and Plonkish proof systems. This means that it will not work with existing circuit compilers out of the box, so advancing this to real-world systems will take additional effort.

- **Swoosh:** Another discussion focused on Swoosh, a protocol designed for efficient lattice-based Non-Interactive Key Exchanges. In an era when we have to rely on post-quantum Key Encapsulation Mechanisms (KEMs) instead of post-quantum Diffie-Hellman based schemes, developing robust key exchange protocols with post-quantum qualities is a strong step forward and a promising area of research.

End-to-end encryption and key transparency

End-to-end (E2E) encryption and key transparency were a significant theme in the conference. A few highlights:

- **Key transparency generally:** Melissa Chase gave a great overview presentation on key transparency's open problems and recent developments. Key transparency plays a vital role in end-to-end encryption, allowing users to detect man-in-the-middle attacks without relying on out-of-band communication.

- **Securing E2EE in Zoom:** Researcher Mang Zhao shared their approach to improving Zoom's E2EE security, specifically protecting against eavesdropping or impersonation attacks from malicious servers. Their strategy relies heavily on Password Authenticated Key Exchange (PAKE) and Authenticated Encryption with Associated Data (AEAD), promising a more secure communication layer for users. They then used formal methods to prove that their approach achieved its goals.

- **E2EE adoption at Meta:** Meta/Facebook stepped up to chronicle their journey in rolling out E2EE on Messenger. Users experience significant friction while upgrading to E2EE, as they suddenly need to take action in order to ensure that they can recover their data if they lose their device. In some cases such as sticker search, Meta decided to prioritize functionality alongside privacy, as storing the entire sticker library client-side would be prohibitive.

Honorable mentions

AEADs: In symmetric cryptography, Authenticated Encryption Schemes with Associated Data (AEADs) were central to discussions this year. The in-depth conversations around Poly1305 and AES-GCM illustrated the ongoing dedication to refining these cryptographic tools. We're preparing a dedicated post about these exciting advancements, so stay tuned!

FHE: The FHE breakout demonstrated the continued progress of Fully Homomorphic Encryption. Researchers presented innovative theoretical advancements, such as a new homomorphic scheme based on Ring Learning with Rounding that showed signs of achieving better performance against current schemes under certain metrics. Another groundbreaking talk featured the HEIR compiler, a toolchain accelerating FHE research, potentially easing the transition from theory to practical, real-world implementations.

The Levchin Prize winners for 2024

Two teams are awarded the Levchin Prize at RWC every year for significant contributions to cryptography and its practical uses.

Al Cutter, Emilia Käsper, Adam Langley, and Ben Laurie received the Levchin Prize for creating and deploying Certificate Transparency at scale. Certificate Transparency is built on relatively simple cryptographic operations yet has an outsized positive impact on internet security and privacy.

Anna Lysyanskaya and Jan Camenisch received the other 2024 Levchin Prize for developing efficient Anonymous Credentials. Their groundbreaking work from 20 years ago is becoming more and more relevant as more and more applications use them.

Moving forward

The Real World Crypto 2024 conference, along with the FHE, RWPQC, and OSCW events, provided rich insights into the state of the art and future directions in cryptography. As the field continues to evolve, with governments, standards bodies, and industry players collaborating to further the nuances of our cryptographic world, we look forward to continued advancements in PQC, E2EE, FHE, and many other exciting areas. These developments reflect our collective mission to ensure a secure future and reinforce the importance of ongoing research, collaboration, and engagement across the cryptographic community.

19.Sui's Fastcrypto Cryptography Library Sets Speed Records

by Mysten Labs
https://blog.sui.io/fastcrypto-speed-benchmarking/

Fastcrypto, the cryptography library used in Sui, has broken many speed records, and our work on benchmarks and security analysis fixed numerous security vulnerabilities while opening the door for innovation by identifying novel optimization tricks.

A paper, Fastcrypto: Pioneering Cryptography Via Continuous Benchmarking, recently presented at the benchmarking workshop of International Conference on Performance Engineering (ICPE) at Imperial College in London, describes our continuous and systematic benchmarking of cryptographic functions in the Fastcrypto library.

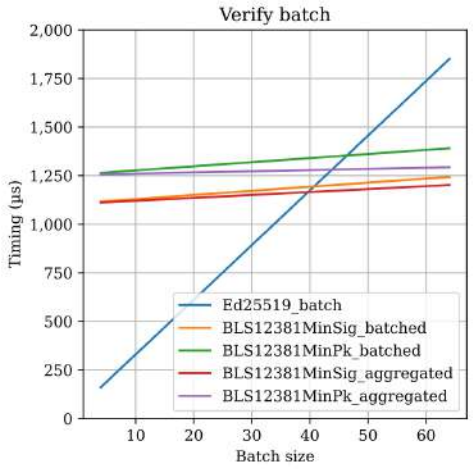
The presentation was part of a session called “Innovations in Performance Testing: Strategies and Technologies” in the Load Testing and Benchmarking of Software Systems workshop. The conference attracted guests from both academia and industry, including representatives from MongoDB and Amazon who also spoke in the same workshop.
We highlighted the systematic and continuous benchmarking of the Fastcrypto library, which is a collection of cryptographic functions such as digital signatures, hash functions, and zero-knowledge proofs. In Fastcrypto, all functions are benchmarked continuously upon release and on-demand, and the results are published online. Similar functions can be easily compared and we maintain the historic data to be able to track performance over time.

The presentation emphasized how these benchmarks have facilitated more informed decision-making in the development of Fastcrypto and Sui, influencing choices of dependencies and usage, as well as optimizing the focus of developer resources.

Qualified decision making from benchmarks

A case study from the paper addressed the challenge of selecting a signature scheme for validators in Sui. For a user to submit a transaction to Sui, the transaction must be signed by a quorum of validators, combined into a transaction certificate. With approximately 100 validators and an equally distributed stake, a quorum consists of 67 validators, meaning each validator must verify 67 signatures per transaction.

The BLS signature scheme allows multiple signatures to be verified as if they were a single signature, but it is a lot slower than alternatives, such as EdDSA. Detailed benchmarking revealed that the break-even point between these two schemes is between 40 and 45 signatures. Hence, for Sui, using BLS is more efficient and this is indeed what is used today.



“You should *also* be worried if the software suddenly is a lot faster”

The presentation also showcased how benchmarks can uncover unexpected software behaviors. One example involved libraries implementing the EdDSA signature scheme, which assumed that the public key should be cached and provided as input to the signing function. If an incorrect public key was provided, it could lead to the extraction of the private key (as shown in our ed25519-unsafe-libs GitHub).

This issue was detected because some libraries exhibited unusually fast performance, bypassing the derivation of the public key and using the potentially incorrect one provided as an argument. While benchmarks often aim to accelerate software, “you should also be worried if the software suddenly is a lot faster,” as noted by an audience member at the workshop.

20.Qubits 2024: D-Wave’s Steady March to Quantum Success

by John Russell

https://www.hpcwire.com/2024/06/18/qubits-2024-d-waves-steady-march-to-quantum-success/

In his opening keynote at D-Wave's annual Qubits 2024 user meeting, being held in Boston, yesterday (17 June 2024) and today, CEO Alan Baratz again made the compelling pitch that D-Wave's brand of analog quantum computing (quantum annealing) is the only quantum technology delivering commercial value today. Many would agree.

- D-Wave's customer base is expanding and at least one customer that has rolled out a second application to production following a successful first deployment.
- Progress on Advantage2, planned to have 7000 qubits, is proceeding on schedule.
- D-Wave continues to roll out improved tools and hybrid solvers that ease application development and deployment.
- It has a paper claiming quantum supremacy that's in peer review and is expected to be published. (There's a pre-press version.)
- D-Wave's gate-based development program, which leverages lessons learned from annealing work, is making progress and D-Wave plans to join the wave of companies offering gate-systems when they are ready – something it doesn't expect soon.

"We are at a watershed moment for quantum computing. We are at the point where quantum computing is transitioning from research experimentation to real business applications in production helping companies to improve their business operations. But there's only one company in the world that can say that, and that's D-Wave Quantum," said Baratz, "And the reason why we can say that is we're the only company in the world that has quantum computers that are large enough and powerful enough to actually be able to support those applications, and we are just now at the point where we are seeing customers actually transition applications into production use."

In practical terms, D-Wave is walking its talk as demonstrated with new collaborations, such as one with Los Alamos National Labs in materials science, new commercial "sales" such as plans announced yesterday by defense contractor Davidson Technology to put a D-Wave system at its Huntsville AL HQ, an expanding international footprint (e.g. Quantum Basel), and solidifying consensus that D-Wave's quantum annealing approach (and analog quantum computing generally) works well on optimization problems. Also, the company's stock (NYSE QBTS) seems relatively stable and recently became part of the Russell 3000 Index.

On the one hand, D-Wave is energized by progress and ambition with chief cheerleader and chief rival critic Baratz leading the charge. On the other hand, Baratz' dogged Rodney Dangerfield-like mantra that 'D-Wave gets no respect' mantra is wearing thin. Maybe that's the nature of the fight.

The war of words over quantum's slippery vernacular — the true meaning of quantum advantage, quantum supremacy, and quantum utility — and trash-talking competitors (if not by name) continues and probably wasn't necessary. Maybe it's mostly a flare to draw attention anyway. One has the sense that Baratz grits his teeth every time he hears a certain three letters of the alphabet and maybe a company named alphabet as well. Time to get over it?

The quantum computing landscape still defies easy description and prediction, but if there is indeed a NISQ (near-term intermediate scale quantum) window for success, D-Wave seems well positioned to grab it. While Baratz unabashedly slammed historic and current criticism of D-Wave Technology, which is his usual practice at these events, he also offered something close to a mild mea culpa in Q&A. Asked how potential users can make sense of the flood of papers, often conflicting, pouring out into the community, he said:

"First of all, we at D-Wave went through a what I'll characterize is a dark period, I don't know, maybe seven or eight years ago, [and] we ended up making some statements that were, frankly overstatements,

and we got slammed very, very hard for doing that. We were just way out in front of our skis, and from that point on, said that we would always be careful, thoughtful, scientifically grounded, measured in everything we do. We would not make a statement or put out a result unless we had confidence that it was scientifically sound and could be backed up.

“Unfortunately, I think, in their desire to demonstrate progress, we’re seeing way too many companies in the quantum space now get out in front of their skis. And unfortunately, since they’re all kind of in it together. They’re not checking one another, and so we end up seeing way too many results and papers that are just overstatements of reality, and we need to stop letting that happen. We need to monitor that. We need to police, that we do it when we see a paper that one of our customers has written on a result using our system, if we can’t repeat it, if we can’t justify it, we’ll say, no, do not talk about this. This is not a solid result. We just need to hold the industry accountable.”

OK, not exactly a mea culpa. Nevertheless, few would disagree that sorting wheat from chaff in the young but high-stakes quantum computing market is difficult at best. For all the time taken to dissect what quantum advantage, quantum supremacy, and quantum utility really mean, or should mean, it’s not really clear that’s a worthwhile effort at this point. The potential user community really doesn’t care – a point made well on a customer panel during the conference about which HPCwire will have coverage later.

They care about applications and ROI versus classical systems (or any other systems).

There wasn’t much breaking ‘news’ but more of a summing up of D-Wave’s plentiful progress since its last Qubits meeting. Much of the material was familiar from its recent analyst day (January 2024). Much of the meat of the conference will come on day-two when sessions will drill down for the user community. (Link to video of keynote. D-Wave will post other recorded sessions next week.)

On the technology front, D-Wave reported steady progress. Its Advantage2 system is expected in 2025/26 time frame; last year, D-Wave launched an 400-qubit prototype, and last quarter introduced a 1200-qubit prototype, each featuring advances. The Advantage2 system will have longer coherence times, 20-way connectivity, and increased energy. In April, D-Wave introduced Fast Anneal protocol on its Leap real-time quantum cloud service.

Baratz said, “We recently launched a new protocol for controlling the quantum computer. It’s called fast anneal. Essentially, what it means is that we can run our annealing algorithm much faster than we were able to run it previously, and, in fact, run it so that most of the time the anneal is running, we’re in the coherent state with the quantum processor.

“The combination of the Advantage2 system and Fast Anneal was what allowed us to demonstrate in Nature 2023 last March, a year ago, that the system is actually performing coherent quantum annealing, and that when the system is performing coherent quantum annealing, we get a scaling polynomial speed up over classical on spin glass optimization problems. It’s also the fast anneal and the 1200 qubit advantage quantum computer that is what has allowed us to achieve the quantum supremacy result, and this is now available in leap for anybody to use as well.”

LANL collaborator Carleton Coffrin, a presenter at the conference, said “When we saw the Advantage2 [announcement] come out, the claim was that it was have higher energy scale, lower noise and better coherence time. Using the protocols we’ve developed over the years for benchmarking these systems, we were able to quickly verify the higher energy scale and a lower noise property. It is difficult to verify the higher coherence time without the Fast Anneal but we’re extremely excited about the release of that feature.

“Since the first paper came out in 2022 we’ve kind of been chomping at the bit to play with it, and now we’re super excited that we have the time to do that. The theoretical physicists at LANL have kind of a

huge list of ideas, and it's going to take us a while to work through them and really do some cool science," said Coffrin.

Customer stories are always a core part of these meeting and D-Wave had several onhand and presenting. GenAI was also significant theme, with presenters from ZapataAI and long-time D-Wave collaborator SavantX tackling the broad topic of blended GenAI-Quantum solutions. You may recall that SavantX developed the Port of Los Angeles application which uses D-Wave's quantum computer. The second half of HPCwire's article, 'Eyes on the Quantum Prize – D-Wave Says its Time is Now', has a fair amount of material on how D-Wave engages customers.)

Collaborators and customers who took the stage with Baratz included:

- ZapataAI (Jon Zorio, CFO) — D-Wave announced the collaboration with ZapataAI in February, "to develop and bring to market commercial applications that combine the power of generative AI and quantum computing technologies."
- Artificial Brain (Dana Linnet, Quantum Market Engagement) — defense an aerospace quantum software specialist. Linnet discussed two applications, including satellite tracking, noting this is an optimization problem that's difficult for classical systems but well suited for D-Wave.
- QuantumBasel (Damir Bogdan, CTO) — An ongoing collaboration which includes providing access to a D-Wave Advantage through QB to Europe-based users.
- Pattison Food (Lindsay Dukowski, senior analytics leader) — Patterson rolled out a scheduling application a year or so go and has added a second.
- Davidson Technologies (Dale Moore, president) — Defense contractor Davidson discussed an application developed for missile defense developed with D-Wave.
- QuantumBasel (Damir Bogdan, CTO) — An ongoing collaboration which includes providing access to a D-Wave Advantage through QB to Europe-based users.
- LANL (Carleton Coffrin, staff scientist) — Unusual magnetism is one of the key focus areas LANL plans to tackle.

It's best to track down the details of these engagements separately and D-Wave is happy to provide them. Most are optimizing programs. Perhaps most impressive were Dukowski's comments on building and deploying a second quantum application. The first application was an ecommerce driver auto scheduling application. The second is for auto scheduling in our stores.

"One of our largest costs is our labor in our stores. So we've been trying, really, for decades, to try to buy a system that could do auto scheduling for us, because that's one of our most manual processes. So we've been looking at top vendors in the space for Workforce Management and scheduling, and they've promised they could do it," said Dukowski. "When we brought them in, they admitted, no, sorry, our environment's pretty complicated. We have over 13 different collective bargaining agreements, unionized environments. The scheduling rules are just too complex to be solved with classical compute.

"The second application we did on our own. It was relatively easy. I have a very talented team. We learned a lot. We had a lot of support with D-Wave, kind of exploring how we could leverage the technology to solve our problems."

Without doubt, D-Wave has faced critics throughout its journey. Clad in a smoking jacket, a top-shelf-beverage nearby, Baratz closed his keynote reading the book of D-Wave, as it were, likening the 25-year race as a tortoise and hare parable.

"This is a story of D-Wave's steady race to a superposition. Once upon a time in a beautiful place where the sea meets the mountains, a quantum computing company was born. D-Wave, from the day it came into existence more than 25 years ago, has had a clear mission to harness the incredible power of quantum technology and put it to use in solving our most challenging problems. It's not the largest or the loudest character, but rather brings a customer focused scientifically validated and ever measured ap-

proach to building successful quantum businesses, much like the Aesop Fable the Tortoise and the Hare," read Baratz.

"D-Wave, the tortoise hasn't always been recognized for its ability to fiercely compete. This is a story of vision, resilience, conflict, execution, and ultimately, success, all the great things that a story needs to have. As with many of our favorite stories, this one is also filled with villains who are eager to take down those they fear, so on its journey to becoming the world's first commercial quantum computing company, D wave has had to fight many battles, slay many dragons and protect the voices of those seeing great outcomes with its solutions."

It was tempting to use the photo above and this part of the Baratz keynote as the introduction to this article. Drama. But even if (still) true, after all this time, the relentless retelling of the story seems less productive now – we get it! – and undermining to the steady one-foot-in-front-of-the-other painstaking progress that has brought D-Wave to the edge of success, at least in the NISQ era. The battle is hardly over.

D-Wave is not the only game in town, although for moving quantum computing into or at least towards production environments, it may well be the farthest along. Neutral atom-based quantum systems, which also currently use an analog approach to QC, are gaining attention and show strength in optimization applications, which Baratz calls the low hanging fruit in QC. Gate-based development by IBM, Google, IonQ, Quantinuum, et al, certainly aren't slowing down but seem further from meaningful revenue goals.

21.Tails 6.4 Anonymous OS Introduces Random Seed to Strengthen All Cryptography

by Marius Nestor
https://9to5linux.com/tails-6-4-introduces-random-seed-to-strengthen-all-cryptography

Tails 6.4 amnesic incognito live system has been released today as the latest stable version of this Debian-based GNU/Linux distribution that protects against surveillance and censorship.

Highlights of Tails 6.4 include the ability to store a random seed on the Tails USB stick to strengthen all cryptography. The devs say that having a secure random number generator is critical for various of Tails' components that rely on cryptography, such as Persistent Storage, Tor, and HTTPS.

"This random seed is stored outside of the Persistent Storage so that all users can benefit from stronger cryptography," reads the release announcement page.

Tails 6.4 also switches to secure HTTPS addresses for the Debian and Tails APT software repositories rather than using onion addresses, updates the Tor Browser anonymous web browser to version 13.0.16, updates the Tor client to version 0.4.8.12, and updates the Mozilla Thunderbird email client to version 115.12.0.

Several bugs were addressed in this update, improving Persistent Storage unlocking, connecting to a mobile network on certain PCs, error messages of Tails Cloner when the target USB stick can't be unmounted because it is being used, and Tor Browser's homepage when using the "New Identity" feature.

On top of that, Tails 6.4 re-enables the PDF reader functionality in the Mozilla Thunderbird app, which was disabled in the previous Tails 6.3 release due to security reasons, and removes the redundant dialog that appears when unlocking a VeraCrypt volume using the Unlock VeraCrypt Volumes utility.

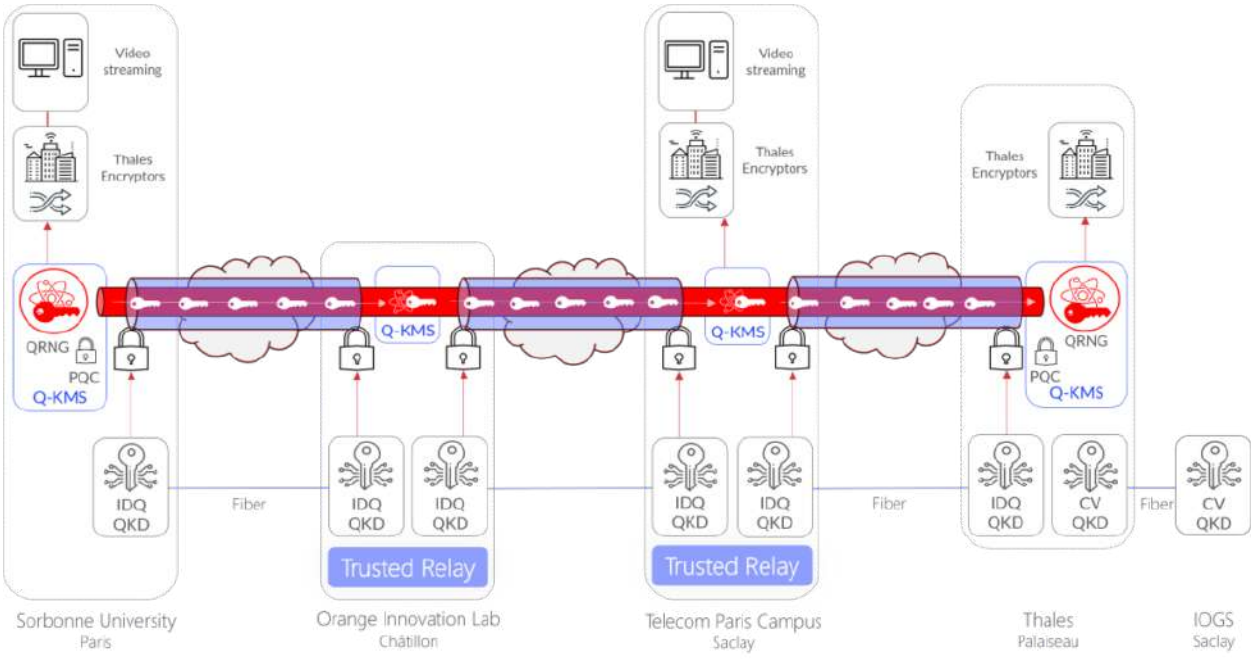
22.PQC-QKD hybridization in Orange's fiber network

by IDQ
https://www.idquantique.com/pqc-qkd-hybridization-in-orange-fiber-network/

The ParisRegionQCI consortium, led by Orange has implemented its first quantum communication network in existing fiber optic infrastructure and we are honored to have contributed to this successful project.

In this demonstration, Quantum Key Distribution (QKD) was implemented on the infrastructure backbone with relays secured by post-quantum cryptography (PQC) to cover an extended distance range in Orange's fiber optic network. The installed solution combines IDQ's commercial Cerberis XG QKD system with embedded Clarion KX software suite (Key Management System), CryptoNext's Quantum Safe Library (C-QSL) and classical symmetric cryptography.

PQC is the next generation of public key cryptography designed to be resistant to quantum computer attacks. In this setup, QKD provides unbreakable key exchange between remote encryption systems, while PQC guarantees relays security in large scale QKD network deployment.



23.D-Wave Introduces New Hybrid Quantum Solver at Qubits 2024 to Tackle Customers' Previously Intractable Workforce, Manufacturing, and Logistics Optimization Problems

by Alex Daigle
https://www.dwavesys.com/company/newsroom/press-release/d-wave-introduces-new-hybrid-quantum-solver-at-qubits-2024-to-tackle-customers-previously-intractable-workforce-manufacturing-and-logistics-optimization-problems/

D-Wave Quantum Inc., a leader in quantum computing systems, software, and services and the world's first commercial supplier of quantum computers, will announce today (17 Jun 2024) at its global Qubits 2024 user conference the launch of a new hybrid quantum solver for nonlinear programs, enabling customers to confront real-world problems of growing complexity. Available now through D-Wave's Leap™ quantum cloud service, D-Wave believes the new solver will help customers solve complex optimization problems of increased scale, pushing past limits of previously available technologies.

The solver supports up to two million variables and constraints, with a tenfold increase in problem size capacity over other D-Wave solvers for certain applications, according to preliminary benchmarking studies. It is part of D-Wave's expanding set of commercial quantum optimization offerings, supporting the company's aggressive go-to-market (GTM) growth strategy announced earlier this year. Comprising a combination of hardware, software and professional services, D-Wave's solutions are designed to dramatically boost time-to-solution for organizations looking to optimize operational processes and performance.

Ready-to-Use Solutions for Workforce, Manufacturing, and Logistics Problems

Real-world problems such as production scheduling have complex interactions between variables. D-Wave's new solver excels at handling nonlinear relationships, where the effect of changes to variables on solution quality is complex, giving it an edge over solvers limited to linear relationships. Its user-friendly experience simplifies the translation of real-world problems into hybrid quantum problem-solving methods, and is exceptionally flexible, supporting a wide range of problems more accurately to deliver better results.

These problems include:

- **Optimized workforce scheduling for improved employee experience:** Industries with large hourly workforces and/or 24/7 operations can implement more streamlined staffing processes, increase productivity, and reduce costs while ensuring compliance with labor laws and employee preferences.

- **Enhanced production scheduling to improve customer satisfaction:** Manufacturers looking to

minimize total completion time and maximize throughput can better meet customer demands by determining the best sequence of tasks in an assembly line — all while considering factors like machine availability, processing times, and due dates.

- **Efficient and more sustainable logistics routing:** Commercial trucking fleets, promotional tour operators, and others seeking to minimize drive time, manage fuel consumption, and address carbon emissions can reduce costs and improve fleet utilization by optimizing routes. According to preliminary internal D-Wave benchmarking studies, the new hybrid quantum solver can find feasible routes for up to 10 times more cities than previous D-Wave solutions when used on a similar scenario — the Traveling Salesperson Problem — a classic example of a challenging combinatorial optimization problem.

Customer Success with Quantum Optimization

Hybrid solvers have been shown to improve solutions to complex optimization problems by bringing together quantum and classical computing resources to explore vast solution spaces more adeptly, and pinpoint answers that are more difficult to calculate than using classical computing methods alone. Over the past year, D-Wave has seen customer use of its hybrid solver portfolio nearly double, which the company believes highlights the growing marketing demand for quantum optimization technology.

“We are confident that this solver will simplify and accelerate customers’ journey to successful quantum technology adoption, helping them more quickly drive return-on-investment, and gain a competitive edge,” said Dr. Alan Baratz, CEO of D-Wave. “Many organizations are recognizing that their most complex computational problems go well beyond the capabilities of existing solutions. They’re adopting hybrid quantum solutions to find better answers to transform operations faster and improve the bottom line.”

“From a logistics standpoint, so many elements go into making our experiences successful. We partnered with D-Wave to tackle the logistics for our large-scale tours and events in a whole new way,” said Jason Snyder, global chief technology officer at Momentum Worldwide. “It's not just about doing things faster or cheaper, but also about being smarter and more sustainable in our approach. For our work, it has helped us make significant progress toward more sophisticated, efficient, and eco-friendly operation models.”

24.Adoption of Composite Signatures Is Major Milestone for Post-Quantum Migration

by Mike Ounsworth and Iain Beveridge
https://securityboulevard.com/2024/06/adoption-of-composite-signatures-is-major-milestone-for-post-quantum-migration/

Hopefully there’s no need for a post-quantum preamble to this blog. Any techies who have not been living in a cave in some outpost of the globe should already be aware of the threat that Cryptographically Relevant Quantum Computers (CRQCs) will have on the classical algorithms that permeate the tech and IT infrastructure that we rely on in the 21st century. Entrust has blogged in the past about Harvest Now, Decrypt Later, with the main takeaway being … you can’t afford to wait until CRQCs are viable.

We also recently blogged on the updates to the Commercial National Security Algorithm Suite (CNSA) 2.0. With an industry eager to start using the new algorithms, the six-year (and counting) NIST PQC competition is nearing a milestone with FIPS 203 and 204 set for publication in the summer of 2024, with FIPS 205 anticipated later in the year.

The concern for some in the industry is that these post-quantum cryptography (PQC) algorithms are shiny and new – mathematically, algorithmically, and in terms of software implementations. In particular, the lattice-based algorithms ML-KEM (FIPS 203) and ML-DSA (FIPS 204) still garner some skepticism about their long-term security.

Enter the hybrids

Hybrids are a combination of a quantum-safe algorithm, such as ML-KEM, with a battle-hardened traditional algorithm, such as RSA or ECDH, to form a "hybrid algorithm." This means any serious threat actor needs to be armed with both a CRQC to break the classical crypto part, and a catastrophic algorithmic breakthrough or implementation bug to break the PQ part. As long as one component remains secure, the data remains secure.

One example of the adoption of the hybrid approach is Hybrid key exchange in TLS 1.3. It's proposed to be the first standardized post-quantum cipher suite for Transport Layer Security (TLS) and builds on years of experimentation with hybrid cipher suites by Google (2016), CloudFlare's TLS Post-Quantum Experiment (2019), and others. It will use the ML-KEM key exchange in combination with an ECDH key exchange.

Entrust has been actively involved in the Internet Engineering Task Force (IETF) working group, with Entrust's John Gray and Mike Ounsworth (co-author of this blog post) being lead authors of a proposed standard that brings the same hybrid encryption protection to network security protocols that use certificate-based encryption, such as S/MIME email encryption: Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS. This proposed internet standard was adopted by the IETF in August 2023 and is well on its way to being published as an RFC.

What about hybrid digital certificates?

When it comes to certificates, the argument in favor of hybrids is less clear. Certificates are most used for authentication. For example, TLS uses certificates mainly for the server to prove that they are who they say they are prior to the user typing in sensitive information. To attack authentication, you need to perform the attack in real time; doing the attack years later does no good. Think of it this way … if a police officer pulls you over and asks for your ID card, you need to produce a real (or forged) card now; the police officer will become impatient if you delay for 10 years until your forging technology has improved!

There are, however, some cases where pre-emptive migration to PQ certificates – and therefore hybrids where the lattice scheme ML-DSA is used –- do provide value. Think, for example, of devices with extremely long service lifetimes that are difficult to upgrade once deployed, such as:

- Satellites in orbit
- Sensors in cars, airplanes, and cell phone towers
- Smart water and electricity meters in people's homes
- The chip in a 10-year ePassport

To push over-the-air firmware updates to these devices, the devices need an embedded cryptographic root to verify the integrity of the new firmware, which leads to the chicken-and-egg problem: What security issues are lurking if you allow field-updating the trusted cryptographic root? Typically, they are

burned into ROM and can't be changed to avoid the whole question.

Therefore, it follows that if you're manufacturing devices that are expected to have a service lifetime beyond "Q-Day," then you should probably be deploying them with PQ (or PQ/traditional hybrid) trusted cryptographic roots today.

With that introduction to the "sometimes urgent, sometimes not" needs for hybrid signatures, let's dive into the world of standards surrounding them.

Entrust recognized as early as 2017 that while hybrid encryption is relatively straightforward, hybrid signatures would need a more elaborate design process. Entrust was involved in the development of one of the earliest post-quantum/traditional (PQ/T) hybrid certificate formats: Multiple Public-Key Algorithm X.509 Certificates, first published in March 2018, and the related mechanism standardized in ITU-T X.509 2019, which has since fallen out of favor for technical reasons.

Major milestone

A new major milestone in the PQ migration journey was recently reached where the IETF adopted Composite ML-DSA for use in Internet PKI, of which John Gray and Mike Ounsworth are also lead authors, into the internet standards track.

This document, the first draft of which was published in March 2019, has seen an incredible amount of community feedback, hackathons, multi-vendor collaboration, academic study, and general debate of all kinds. It failed its first call-for-adoption in June 2023, mainly due to the scope of the document being too broad. With a few more rounds of industry feedback to distill it down to the core elements, it passed its second call-for-adoption on May 1, 2024.

Reassuring IETF-backed standards

At Entrust, we know that X.509 certificates and public key infrastructure is more than HTTPS certificates. We know that next to TCP/IP, X.509 certificates are one of the oldest and most fundamental technologies of the internet, providing the trust layer that underpins a vast diversity of network security protocols.

Looking to the long tail of specialized uses of X.509 as we help our customers migrate to PQ over the coming decade, we're pleased to have IETF-backed standards for both composite encryption and PQ composite signatures in our toolbox. Learn more about our post-quantum cryptography solutions.

25.Estonia's Roadmap for Encryption in the Age of Quantum Computing

by James Dargan
https://thequantuminsider.com/2024/06/13/estonias-roadmap-for-encryption-in-the-age-of-quantum-computing/

The emergence of powerful quantum computers poses an existential threat to today's encryption systems. At the Future Cryptography Conference in Tallinn, Estonia, cryptography expert Jan Willemson provided insights into when and why we need to transition to post-quantum cryptography (PQC) to maintain data security.

Willemson began by explaining the rationale for cryptography: “The state is needed so that citizens could be provided with services. We want these services to be available to those who need them.” He stressed properties like fairness, accountability and privacy that citizens expect from state services, which cryptography helps enable.

On the quantum computing threat, Willemson cited research estimating breaking 2048-bit RSA keys could take “about 100 days under ideal conditions” or “years perhaps even decades under more realistic conditions” with a large quantum computer. While much faster than classical computing, he noted “it’s still some significant amount of time involved so it’s not like you will break it in a blink of an eye.”

Willemson outlined three areas where pre-quantum cryptography may suffice even after large quantum computers emerge based on risk analysis.

“If your confidentiality horizon is less than the time that it would take to break the encryption key then it might actually be okay to use pre-quantum encryption,” he said.

He mentioned that if the value of a signature is less than the cost of breaking a key, then it is actually acceptable to use pre-quantum signatures. He also noted that authentication typically occurs for one session and for a limited time, implying that in many scenarios, using pre-quantum authentication may be quite adequate.

However, he cautioned “you don’t always know the future value of all your signatures” which could retroactively incentivize attacks, suggesting “it may be justified to convert to post-quantum crypto just in case.”

Willemson described Estonia’s progress: “The encryption part of the internet voting system is completely under our control, so we define what crypto system we use—this part is going to be much easier to upgrade.”

As nations prepare for the quantum era, an open, transparent process is crucial according to Willemson.

“NIST realizes this very well and this is a reason why for a few decades they already now are running very open competitions,” he said.

With pragmatic risk analysis and strategic implementation across vital systems, Estonia is pioneering the “quantum leap” to quantum-resistant cryptography.

26.The South African who helped end apartheid with encryption and inspired a Hollywood movie

by Jan Vermeulen
https://mybroadband.co.za/news/security/540163-the-south-african-who-helped-end-apartheid-with-encryption-and-inspired-a-hollywood-movie.html

Former political prisoner and old-school hacker Tim Jenkin co-developed and built an encrypted electronic communications network in the 1980s that became a vital instrument in ending apartheid.

Years earlier, Jenkin and two other inmates had escaped from Pretoria Central Prison by reverse-engineering the keys of ten separate doors (and some extras) from wood.

Jenkin and university friend Stephen Lee landed in jail after joining the ANC in 1974 and setting off pamphlet bombs with anti-apartheid messaging in Cape Town between 1975 and 1978.

Former ANC spymaster Ronnie Kasrils said in the documentary *The Vula Connection* that Jenkin held the record for detonating 18 or 19 leaflet bombs in the Cape Town city centre in one day.

He said Jenkin and Lee weren't the usual intellectual types who joined the ANC as students. They combined brains with industriousness.

Jenkin had the extra advantage of being unassuming and almost withdrawn. "Which is exactly what you want," Kasrils added.

Unfortunately, the security police soon had the pair under surveillance. They were arrested at 03:00 on 2 March 1978 while moving their printing equipment.

Under legal advice, they pleaded guilty to all charges. Jenkin was sentenced to twelve years in prison and Lee to eight.

Within 18 months, they had broken out. The caper became the subject of the 2020 film *Escape from Pretoria*, with Harry Potter star Daniel Radcliffe portraying Jenkin. By early 1980, Jenkin had relocated to London and was assigned to training operatives in the encryption techniques they needed in the field.

The ANC used a simple but effective paper-based one-time pad system for cryptography, which Jenkin trained recruits in.

One-time pad relies on single-use keys that must be pre-generated and issued to a group of communicating parties.

As messages are encrypted and decrypted, the keys are consumed and should not to be reused.

While the encryption itself is uncrackable, provided keys are properly randomly generated, one-time pad systems have several other vulnerabilities.

If an adversary gets their hands on the pre-generated keys and are able to intercept every message from then on, they can decrypt them.

Operatives must also adhere to strict operational security protocols, such as destroying decrypted messages, old key pages, and old enciphered messages.

However, the main problem, Jenkin found, was that encryption and decryption was laborious.

"It took so much effort to say so very little and the responses, as few and far between as they were, contained little encouragement and advice," he said.

"There were only instructions which usually lacked any connection with the reality they were experiencing."

This quickly demoralised new operatives, and Jenkin said he could see their enthusiasm and activity rapidly die.

In the early eighties, computers were getting cheaper, and Jenkin believed a program to automate the cryptography could solve their communications problem.

Together with new partner-in-crime Ronnie Press, they began work on a system that would eventually become a fully-fledged underground electronic communications network.

“Off to the bookshops and libraries I went to find out about secure encryption algorithms,” Jenkin said.

“Nothing impressed me very much and all I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists.”

While he did learn a few tricks they could use, he decided to keep it simple and digitise their existing one-time pad system.

Although their cryptography would remain simple, the whole communications system ended up having a lot more moving parts than just the software, as most of the Internet did not yet exist.

To transmit encrypted messages, they were encoded into a signal that could be played over a regular telephone call and recorded. This was to allow operatives to easily receive messages via public telephones.

The recorded message could then be played back into a computer via a modem and decrypted.

However, keys had to be distributed to the two communicating parties to encrypt or decrypt messages.

For this, Jenkin wrote random data to 1.44MB “stiffy” disks. These keys and the encryption program itself then had to be delivered to operatives in the field.

Enter Conny Braam, head of the Dutch anti-apartheid movement, who found a KLM air hostess sympathetic to their cause.

The hostess, Antoinette Vogelsang, helped smuggle the computers, disks, and other equipment ANC operatives in South Africa needed.

Vogelsang’s role was critical if the system was going to work. Had she provided copies of the disks to the South African authorities, the whole endeavour would have been compromised.

With everything in place, the ANC kicked off Operation Vula.

They infiltrated key leaders like Mac Maharaj, Siphiwe Nyanda, and Charles Nqakula back into South Africa with the ability to communicate with one another and the ANC headquarters in exile. Kasrils would later join them.

In 1989, the system and Operation Vula would achieve its greatest victory — re-establishing secure communications between Nelson Mandela in South Africa and ANC president Oliver Tambo in Lusaka, Zambia.

Mandela had been transferred to house arrest as part of negotiations to transition to a democratic South Africa.

However, the apartheid government kept Mandela isolated from the rest of the ANC in the hopes of securing more favourable terms by creating the impression they were negotiating solely with him.

While it was not possible to smuggle a computer and disks to Mandela, messages were relayed in the

covers of books.

Mandela's replies could then be smuggled out, encrypted using the software, and transmitted to Tambo in Lusaka.

"Messages from Mandela became a regular feature and in response there were long memos from Oliver Tambo in Lusaka," said Jenkin.

"The two were now talking in confidence for the first time since the early 60s."

27.IDEMIA and seven French cybersecurity leaders unite for quantum security solutions

by Kajal Mehra
https://timestech.in/idemia-and-seven-french-cybersecurity-leaders-unite-for-quantum-security-solutions/

As the cybersecurity landscape evolves with the looming threat of quantum computing, industry leaders are joining forces to develop robust solutions. The Hyperform consortium unites several leading players in cybersecurity and post-quantum: IDEMIA Secure Transactions, project coordinator and a leading provider of secure solutions, CryptoNext, a provider of post quantum cryptography remediation solutions, Atempo. a provider of data protection solutions, Prim'X, a software publisher of encryption solutions, Synacktiv, an offensive security company and licensed testing laboratory (CESTI), CEA Leti, a global leader in miniaturization technologies enabling smart, energy-efficient and secure solutions for industry, INRIA, the French national institute for digital science and technology, with world-class researchers in cryptography and secure implementation, and the French cybersecurity agency (ANSSI), who will supervise the security and performance assessment of the solution.

Funded by the French government investment plan France 2030, and credits from the European Union, the consortium is a key element in the development of European sovereignty in post-quantum cryptography.

A sovereign quantum-safe offering at the forefront of global industrial research

The arrival of the quantum computer will jeopardize the security of sensitive data. The objective of Hyperform is to design quantum-safe solution that will protect government, enterprise and citizen data from the threat of quantum computer. The consortium will set up a complete demonstrator for cloud data storage, documents archiving and online collaboration, based on sovereign encryption software used to protect the most critical information.

With more than 7.5 million euros invested by the consortium, France 2030 and the European Union, and 29 experts recruited, the Hyperform consortium has very strong ambitions. Over the next three years, the Hyperform consortium will work to develop quantum-safe components so that service providers – including banks, governments, and software companies – can ensure unrivalled data security for their end-user services. The first end-to-end solutions will have the potential to set the standard for the whole industry.

As part of this project, the consortium will develop a next generation quantum-safe chip and create post-quantum cryptographic libraries, enhancing payment transactions as well as identity document reading.

In order to facilitate the transition to these advanced security measures, existing cybersecurity software will be modified. The performance and security of these new solutions will be assessed under the supervision of the ANSSI security agency.

“True to our commitment to provide service providers with state-of-the-art security services, we are very proud to lead the Hyperform consortium. This collaborative project highlights our shared expertise in post-quantum technologies and our joint commitment to crafting solutions that meet industry demands. By working hand-in-hand with the ecosystem, we will be able to develop a robust quantum-safe framework, driving co-innovation and industry-wide progress,” says **Marc BERTIN, Chief Technology Officer at IDEMIA Secure Transactions.**

With a global team of 800 experts in research and development, IDEMIA Secure Transactions stands at the forefront of technology, particularly in post-quantum cryptography, as a world-leading authority. The company has been a trailblazer in the advancement of post-quantum algorithms and notably, in 2022, achieved a milestone by introducing the first quantum-resistant 5G SIM. The Division recently unveiled the first crypto-agility solution that will enable service providers of secure products to future-proof the security of their products in the post-quantum era.

28.Researchers Use Quantinuum’s New 56-Qubit Quantum Computer To Show 100X Improvement On Google’s 2019 Random Circuit Sampling Task

by Matt Swayne
https://thequantuminsider.com/2024/06/05/researchers-use-quantinuums-new-56-qubit-quantum-computer-to-show-100x-improvement-on-googles-2019-random-circuit-sampling-task/?utm_source=newsletter&utm_medium=email&utm_term=2024-06-08&utm_campaign=TQI+Weekly+Newsletter+--+For+Quantinuum+s+New+QC+Microsoft+MegaCommitment+Plus+More+Quantum+News+Industry+Updates

Quantinuum, the world’s largest integrated quantum computing company, today unveiled the industry’s first quantum computer with 56 trapped-ion qubits. H2-1 has further enhanced its market-leading fidelity and is now impossible for a classical computer to fully simulate.

A joint team from Quantinuum and JPMorgan Chase ran a Random Circuit Sampling (RCS) algorithm, achieving a remarkable 100x improvement over prior industry results from Google in 2019 and setting a new world record for the cross entropy benchmark. H2-1’s combination of scale and hardware fidelity makes it difficult for today’s most powerful supercomputers and other quantum computing architectures to match this result.

“We’re extending our lead in the race towards fault tolerant quantum computing, accelerating research

for customers like JPMorgan Chase in ways that aren't possible with any other technology," said Rajeeb Hazra, CEO of Quantinuum**.** "Our focus on quality of qubits versus quantity of qubits is changing what's possible, and bringing us closer to the long-awaited commercialization of quantum's applications across industries like finance, logistics, transportation and chemistry."

According to Ilyas Khan, founder and Chief Product Officer, Quantinuum**,** the experiment shows that quantum is moving from the theoretical to the applied and from the scientific to the practical, according to Ilyas Khan, founder and Chief Product Officer, Quantinuum.

Khan said: "When, in late 2019, Google released details of their 'quantum supremacy' experiment, Sundar Pichai their CEO published a blog that has withstood the test of time with respect to the importance of the milestone that was then reached. Our work, published today, and done in collaboration with researchers from JP Morgan, Argonne National Labs and Caltech, elevates that bar to one where we clearly now operate in a place that has been anticipated for so long. One where classical supercomputers simply cannot compete and where the computational task is measurable and relevant. I could not be more excited to share this with the quantum eco-system as a whole, with great pride and also with further anticipation as we have disclosure lined up over summer that will continue to extend our lead as we build scalable universal fault tolerant quantum computers."

Quantinuum's analysis also indicates that the H2-1 executes RCS at 56 qubits with an estimated 30,000x reduction in power consumption compared to classical supercomputers, reinforcing it as the preferred solution for a wide array of computational challenges.

"The fidelity achieved in our random circuit sampling experiment shows unprecedented system-level performance of the Quantinuum quantum computer. We are excited to leverage this high fidelity to advance the field of quantum algorithms for industrial use cases broadly, and financial use cases in particular," said Marco Pistoia, Head of Global Technology Applied Research at JPMorgan Chase.

Today's announcement is the latest in a string of breakthroughs made by Quantinuum in 2024:

- In March, the company revealed a long-sought solution to the "wiring problem," demonstrating that the quantum charge-coupled device (QCCD) architecture can scale to large qubit numbers.
- Quantinuum's H-Series became the first to achieve "three 9s" – 99.9% – two-qubit gate fidelity across all qubit pairs in a production device, a critical milestone enabling fault-tolerance.
- Then, in collaboration with Microsoft, Quantinuum 's H2-1 was declared the first – and so far the only – quantum computer capable of achieving Level 2 Resilient quantum computing, creating four reliable logical qubits using error correction and detection to achieve an 800-fold reduction in error rate.

"Microsoft looks forward to a continued collaboration with Quantinuum as they release their high fidelity 56-qubit machine," said Dennis Tom, General Manager Microsoft Azure Quantum**.** "Recently, the teams created four highly reliable logical qubits by applying Azure Quantum's qubit-virtualization system to Quantinuum's 32-qubit machine. With the additional physical qubits available on Quantinuum's new machine, we anticipate creating more logical qubits with even lower error rates. As we reach these milestones, we will continue to increase the resiliency of quantum operations as well as the utility of quantum computing."

Quantinuum also recently closed a $300 million equity fundraise anchored by JPMorgan Chase with additional participation from Mitsui & Co., Amgen and Honeywell, which remains the company's majority shareholder, bringing the total capital raised by Quantinuum since inception to approximately $625 million.

29.KT Completes Commercialization-Ready Post-Quantum Cryptography Solution

by Jung So-yeon
https://www.koreaittimes.com/news/articleView.html?idxno=131998

KT announced on June 5th that it has completed preparations for the commercialization of post-quantum cryptography (PQC) technology.

PQC is a new public key cryptographic method designed to address the threats posed to existing encryption systems by advancements in quantum computing. It uses complex mathematical algorithms that would take even high-performance quantum computers billions of years to crack.

KT independently developed the standalone model of the QENC (Quantum ENCrytor), a quantum encryption communication device, and designed the PQC solution service through technology transfer. The KT PQC solution can utilize both encryption keys generated by a quantum key distribution (QKD) device and keys generated by the PQC algorithm, enabling the creation of a hybrid quantum security network.

A hybrid quantum security network combines quantum key distribution (QKD) technology, which fundamentally blocks eavesdropping attempts on physical lines, with PQC, which provides security that even quantum computers cannot decrypt. This dual security method significantly enhances safety. Additionally, it provides encryption functions for a variety of service interfaces based on user needs, supporting network equipment speeds of 1G/10G/100G.

The external key interface of KT's QENC is designed in compliance with the international standard ETSI GS QKD 014 based on open interfaces. Therefore, using an external PQC key is possible by simply connecting to the PQC server without needing to change the encryption device.

The connection to an external PQC key enhances security by applying TLS1.3, used for secure internet communication. Since it receives keys from a separate PQC server, it can quickly respond to national security requirements. Furthermore, KT has applied the NIST standard PQC algorithms CRYSTALS-Dilithium and CRYSTALS-Kyber, which strengthens data security.

In South Korea, public institutions need to pass a security suitability verification to use quantum encryption communication devices. KT's QENC equipment submitted for a security function confirmation test last May is expected to receive the security function confirmation certificate by July, allowing it to be utilized by all domestic institutions.

KT Enterprise's Data Business Head, Seung-Taek Baek, stated, "With the commercialization of the hybrid standalone QENC device and the PQC solution, KT aims to continue its role as a leading player in the activation of the domestic quantum encryption communication market."

30.TII McEliece Encryption Challenges winners revealed

https://mystartupworld.com/tii-mceliece-encryption-challenges-winners-revealed/

The Technology Innovation Institute (TII) has announced the winning submissions for the TII McEliece Challenges, the United Arab Emirates' cryptography challenges that aim to enhance online security and encourage advancements in cryptographic systems.

The McEliece cryptosystem is a public key encryption scheme with a strong reputation for being resilient to cyberattacks. As part of the challenges, cryptographers, mathematicians, innovators, research institutes, and university students were invited to validate the security of the cryptosystem to identify possible weaknesses and confirm its strength. Cryptography ensures the confidentiality of information thanks to the encryption of data, which is crucial to cybersecurity.

Participants had to solve four challenges launched by the TII, a leading global scientific research center and the applied research pillar of Abu Dhabi's Advanced Technology Research Council (ATRC).

The Rocco Mora from France; Lorenz Panny, assistant professor at the Technical University Munich; and Run Timerr from Sweden were the winners taking home cash prizes totaling $22,000.

TII CEO, Dr. Najwa Aaraj, applauded the winners, and said: "By delving into the intricacies of the McEliece-based cryptosystem, we deepened our understanding of it and increased the confidence in its security."

TII kicked off the year-long competition in May 2023, via HeroX, a crowdsourcing platform focused on problem solving challenges. The challenges featured multiple McEliece-based cryptanalysis problems with increasing levels of difficulty exploring four different tracks: Track 1A on Theoretical Key Recovery Algorithms, Track 1B on Practical Key Recovery, and Track 2A and 2B on Message Recovery.

Three out of the four prizes were awarded, while the hardest challenge in Track 2B remained expectedly unbroken. The three prizes were given to the best judged submission in Track 1A and to the researchers who solved the most difficult instances in Track 1B and Track 2A.

The McEliece cryptosystem has become a leading choice among code-based cryptosystems for standardization by the National Institute of Standards and Technology (NIST).

The winning individuals and teams are as follows:

Track 1A – Theoretical Key Recovery

The prize for the theoretical Track 1A was awarded to the Rocco Mora from France. The submission provides a novel theoretical to distinguish McEliece public keys from random data for some parameter instances of the cryptosystem. The ideas developed in the submission are intriguing and appealing for further developments. It significantly improves the state-of-the-art distinguishers for alternate codes that are central to the McEliece cryptosystem. The winners have been awarded the full prize of U$10,000.

Track 1B – Practical Key Recovery

Lorenz Panny, assistant professor at the Technical University Munich, has secured the winning position by successfully recovering the secret key for an instance with a previously estimated security level of 83 bits. This remarkable achievement has earned him the full prize of US$10,000. Panny utilized a combination of a partial key enumeration technique and an optimized version of the Support Splitting Algorithm to identify correct guesses. His work sheds light on potential overestimations of security levels in provided instances, promising a more accurate estimation of attack costs. He plans to provide a detailed description of his techniques and prepares for the publication of his source code, which will further con-

tribute to the community's understanding of the security of the McEliece cryptosystem.

Track 2A – Message Recovery

Last but not least, we congratulate Run Timerr from Sweden for securing a US$2,000 prize for successfully decrypting a McEliece ciphertext (without knowledge of the secret key), estimated to a complexity of about 60 bits for the solved instance. Timerr used an optimized implementation of Stern's Information Set Decoding algorithm provided by Daniel Bernstein, Tanja Lange and Christiane Peters.

31.ARPA Network nets $6M to support cryptographic AI based on biometrics, ZKML

by Joel R. McConvey
https://www.biometricupdate.com/202406/arpa-network-nets-6m-to-support-cryptographic-ai-based-on-biometrics-zkml

ARPA Network, a blockchain-agnostic Layer-2 computation network that develops cryptographic systems to enable more blockchain use cases, has secured $6 million in strategic investment led by Nomura subsidiary Laser Digital and web3 VC firm DeFiance Capital. A release from the company says the funds will support product expansion in fully on-chain gaming, Autonomous Worlds (AW), and cryptographic AI.

"This infusion of capital from industry leaders marks a milestone for ARPA," says Felix Xu, co-founder of ARPA Network. "Together with leading AI institutions, we will publish research and conduct PoC on cryptographic AI for facial recognition using zero-knowledge machine learning (ZKML)."

ZKML is a system that can perform computations off-chain and provide proof that said computations were correctly executed, while limiting shared private data. Verifying the proof on-chain exacts a much smaller computational cost than doing the initial computation. Therefore, the system makes scaling possible. (On Medium, Bastian Wetzel offers a good primer on ZKML.)

Aiming for on-chain, privacy-preserving biometric tech that gives users easy and secure access to the blockchain, ARPA's proof of concept on cryptographic AI for facial recognition using ZKML exploits the crossover of cryptography and AI to expand blockchain capabilities and – in theory – lower the barrier to mass adoption.

Laser Digital CEO Jez Mohideen says "ARPA's initiatives in on-chain gaming and cryptographic AI are poised to transform the blockchain landscape, making these technologies more accessible and impactful across various industries." He says the investment underlines his firm's dedication to "enhancing the digital landscape and supporting technologies that offer significant market potential and align with our values of responsible innovation."

According to Arthur Cheong, CIO of DeFiance Capital, ARPA's decentralized tech "is vital not only for fully on-chain games but also for enhancing the reliability and privacy of applications across the entire blockchain space." Much enthusiasm, however, is directed at ARPA's first foray into fully on-chain game, DEAR – a "smart-contract-based creature living on-chain" that "challenges players to nurture, influence,

and ultimately shape the digital lifeform through interactions."

The description may trigger fond memories for those who grew up during the Tamagotchi craze of the late 1990s. But the stated goal is loftier than providing a digital pocket pet, aiming to establish fully on-chain gaming as a platform offering high levels of engagement and fairness.

Additional support for the funding round comes from Animoca Ventures, Metrics Ventures, ArkStream Capital and Trinito.

World ID project among those pushing zero-knowledge proofs

ARPA Network is not the only organization to stump for cryptographic digital ID as an alternative to other forms of remote identity verification. Steven Smith, head of protocol for Worldcoin parent company Tools for Humanity, has gone on record saying deepfake technology has made selfie biometrics unreliable for identity verification. Indeed, Worldcoin's website hosts a detailed breakdown of ZKML.

Yet while Smith notes the value of blockchain and zero-knowledge proofs for securely proving claims, he also concedes that these two tools alone are insufficient to provide reliable proof of humanity – Worldcoin's identity holy grail. Hence the firm's use of iris biometrics to complete the picture.

32.Cryptographers Discover a New Foundation for Quantum Secrecy

by Ben Brubaker
https://www.quantamagazine.org/cryptographers-discover-a-new-foundation-for-quantum-secrecy-20240603/

Say you want to send a private message, cast a secret vote or sign a document securely. If you do any of these tasks on a computer, you're relying on encryption to keep your data safe. That encryption needs to withstand attacks from codebreakers with their own computers, so modern encryption methods rely on assumptions about what mathematical problems are hard for computers to solve.

But as cryptographers laid the mathematical foundations for this approach to information security in the 1980s, a few researchers discovered that computational hardness wasn't the only way to safeguard secrets. Quantum theory, originally developed to understand the physics of atoms, turned out to have deep connections to information and cryptography. Researchers found ways to base the security of a few specific cryptographic tasks directly on the laws of physics. But these tasks were strange outliers — for all others, there seemed to be no alternative to the classical computational approach.

By the end of the millennium, quantum cryptography researchers thought that was the end of the story. But in just the past few years, the field has undergone another seismic shift.

"There's been this rearrangement of what we believe is possible with quantum cryptography," said Henry Yuen, a quantum information theorist at Columbia University.

In a string of recent papers, researchers have shown that most cryptographic tasks could still be accomplished securely even in hypothetical worlds where practically all computation is easy. All that matters is the difficulty of a special computational problem about quantum theory itself.

"The assumptions you need can be way, way, way weaker," said Fermi Ma, a quantum cryptographer at the Simons Institute for the Theory of Computing in Berkeley, California. "This is giving us new insights into computational hardness itself."

This Message Will Self-Destruct

The story begins in the late 1960s, when a physics graduate student named Stephen Wiesner started thinking about the destructive nature of measurement in quantum theory. Measure any system governed by the rules of quantum physics, and you'll alter the quantum state that mathematically describes its configuration. This quantum measurement disturbance was a hindrance for most physicists. Wiesner, who took an unorthodox information-centric view of quantum theory, wondered whether it could be made useful. Perhaps it could serve as a form of built-in tamper protection for sensitive data.

But Wiesner's ideas were too far ahead of their time, and he left academia after graduate school. Fortunately, he'd discussed his ideas with his friend and fellow physicist Charles Bennett, who unsuccessfully tried to interest others in the subject for a decade. Finally, in 1979, Bennett met the computer scientist Gilles Brassard while swimming off the coast of Puerto Rico during a conference. Together, they wrote a groundbreaking paper describing a new approach to an important cryptographic task. Their protocol was based on quantum measurement disturbance, and needed no assumptions about the difficulty of any computational problems.

"The very nature of quantum information seems somewhat cryptographic," Ma said.

Bennett and Brassard's breakthrough made researchers optimistic that similar quantum tricks could yield perfect security for other cryptographic tasks. Researchers focused mainly on a task called bit commitment, which is useful on its own and is also a key component of most advanced cryptographic protocols.

To understand the basic idea behind bit commitment, imagine a two-player game in which you must make a secret decision that later gets revealed. One way to do this is to write the decision down on a slip of paper and put it in a sealed envelope. That way, you can't change your decision later on, and your opponent can't prematurely peek at the result.

Now imagine you're playing the same game online. To make cheating impossible, you need to seal the decision in a sort of digital envelope that neither player can open alone. That's where cryptography comes in. In 1981, the pioneering computer scientist Manuel Blum constructed the first bit commitment protocol — a way to build effectively unhackable envelopes out of hard computational problems.

But how hard is hard? Researchers in the field of computational complexity theory study many different kinds of hard problems, and not all of them are useful for cryptographers. Bit commitment and all other cryptographic protocols rely on problems in a class that complexity theorists call "NP," whose defining feature is that it's easy to check whether a candidate solution is correct.

Unfortunately, researchers haven't been able to prove that any NP problems are truly hard. There could still be some clever undiscovered procedure, or algorithm, for solving even the ones that seem hardest. If there is, then all of classical cryptography would break.

Such considerations animated the search for quantum-based security guarantees. But in 1997, two papers proved that bit commitment schemes could never be completely secure if they were based solely on the laws of quantum physics. The papers implied that some kind of computational hardness would be necessary for almost all cryptographic tasks.

That was the last word on the theoretical foundations of quantum bit commitments for nearly 25 years.

Then, in 2021, a paper by a graduate student named William Kretschmer prompted researchers to confront a question that nobody had thought to ask. Computational hardness was clearly necessary for bit commitments and most other forms of cryptography, but precisely what kind of hardness?
.
.
.

33.NIST Q&A: Getting Ready for the Post Quantum Cryptography Threat? You Should be.

by John Russell
https://www.hpcwire.com/2024/06/03/nist-qa-getting-ready-for-post-quantum-cryptography-threat-you-should-be/

With the National Institute of Standards and Technology (NIST) set to publish the first Post Quantum Cryptography (PQC) Standards in a few weeks, attention is shifting to how to put the new quantum-resistant algorithms into practice. Indeed, the number of companies with practices to help others implement PQC is mushrooming and contains familiar (IBM, Deloitte, et al.) and unfamiliar names (QuSecure, SandboxAQ, etc.).

The Migration to Post-Quantum Cryptography project, being run out of NIST's National Cybersecurity Center of Excellence (NCCoE), is running at full-tilt and includes on the order of 40 commercial participants.

In its own words, "The project will engage industry in demonstrating use of automated discovery tools to identify all instances of public-key algorithm use in an example network infrastructure's computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms. The algorithm employed and its purpose would be identified for each affected infrastructure component."

Getting to that goal remains a WIP that started with NIST's PQC program in 2016. NIST scientist Dustin Moody leads the PQC project and talked with HPCwire about the need to take post quantum cryptography seriously now, not later.

"The United States government is mandating their agencies to it, but industry as well as going to need to be doing this migration. The migration is not going to be easy [and] it's not going to be pain free," said Moody, whose Ph.D. specialized in elliptic curves, a commonly used base for encryption. "Very often, you're going to need to use sophisticated tools that are being developed to assist with that. Also talk to your vendors, your CIOs, your CEOs to make sure they're aware and that they're planning for budgets to do this. Just because a quantum computer [able to decrypt] isn't going to be built for, who knows, maybe 15 years, they may think I can just put this off, but understanding that threat is coming sooner than than you realize is important."

Estimates vary wildly around the size of the threat but perhaps 20 billion devices will need to be updated with PQC safeguarding. NIST has held four rounds of submissions and the first set of standards will encompass algorithms selected the first three. These are the main weapons against quantum decryption

attack. The next round seeks to provide alternatives and, in some instances, somewhat less burdensome computational characteristics.

The discussion with Moody was wide-ranging, if perhaps a little dry. He covers PQC strategy and progress and the need to monitor the constant flow of new quantum algorithms. Shor's algorithm is the famous threat but others are percolating. He notes that many submitted algorithms broke down under testing but says not to make much of that as that's the nature of the standards development process. He talks about pursuing cryptoagility and offers a few broad tips on preparation.

Moody also touched on geopolitcal rivalries amid what has been a generally collaborative international effort.

"There are some exceptions like China never trusting the United States. They're developing their own PQC standards. They're actually very, very similar to the algorithms [we're using] but they were selected internally. Russia has been doing their own thing, they don't really communicate with the rest of the world very much. I don't have a lot of information on what they're doing. China, even though they are doing their own standards, did have researchers participate in the process; they hosted one of the workshops in the field a few years back. So the community is small enough that people are very good at working together, even if sometimes the country will develop their own standards," said Moody.

How soon quantum computers will actually be able to decrypt current RSA codes is far from clear, but early confidence that would be many decades has diminished. If you're looking for a good primer on the PQS threat, he recommended the Quantum Treat Timeline Report released in December by the Global Risk Institute (GRI) as one (figures from its study below).

HPCwire: Let's talk a little bit about the threat. How big is it and when do we need to worry

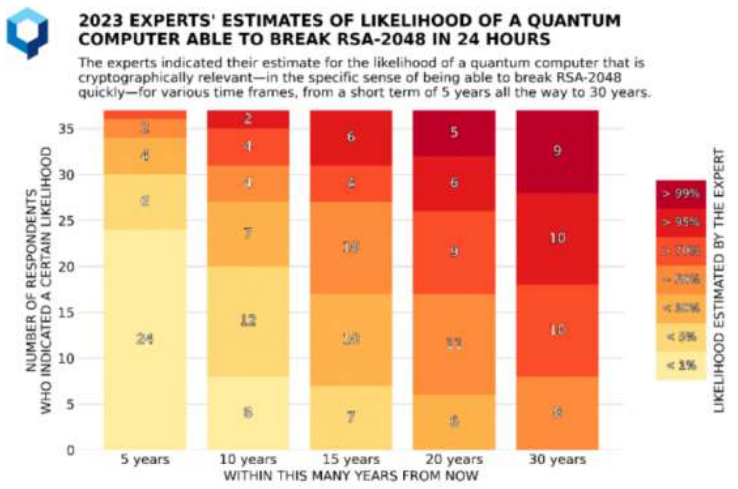
Dustin Moody: Well, cryptographers have known for a few decades that if we are able to build a big enough quantum computer, it will threaten all of the public key crypto systems that which we use today. So it's a it's a serious threat. We don't know when a quantum computer would be built that's large enough to attack current levels of security. There's been estimates of 10 to 15 years, but you know, nobody knows for certain. We have seen progress in companies building quantum computers — systems from IBM and Google, for example, are getting larger and larger. So this is definitely a threat to take seriously, especially because you can't just wait until the quantum computer is built and then say now we'll worry about the problem. We need to solve this 10 to 15 years in advance to protect your information for a long time. There's a threat of harvest-now-decrypt-later that helps you understand that.

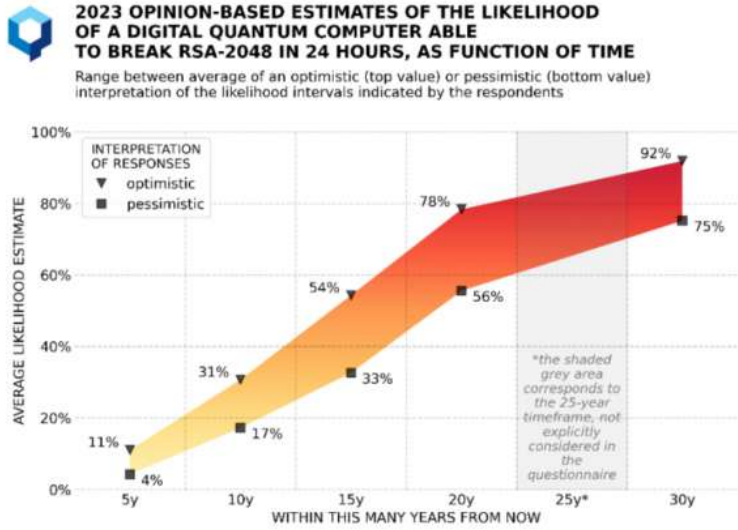
HPCwire: Marco Pistoia, who leads quantum research for JPMorgan Chase, said he'd seen a study suggesting as few as 1300 or so logical qubits might be able to break conventional RSA code, although it would take six months to do so. That was a year ago. It does seem like our ability to execute Shor's algorithm on these systems is improving, not just the brute force, but our cleverness in getting the algorithm to run.

Dustin Moody: Yep, that's true. And it'll take a lot of logical qubits. So we're not there yet. But yeah, progress has been made. You have to solve the problem solved and migrate to new solutions before we ever get to that point,

HPCwire: We tend to focus on Shor's algorithm because it's a direct threat to the current encryption techniques. Are there others in the wings that we should be worried about?

Dustin Moody: There's a large number of quantum algorithms that we are aware of, Shor being one of them, Grover's being another one that has an impact on cryptography. But there's plenty of other quantum algorithms that do interesting things. So whenever anyone is designing the crypto system, they have to take a look at all those and see if they look like they could attack the system in any way? There's kind





of a list of I don't know, maybe around 15 or so that potentially people have to kind of look at him and figure out, do I need to worry about these.

HPCwire: Does NIST have that list someplace?

Dustin Moody: There was a guy at NIST who kept up such a list. I think he's at Microsoft, now. It's been a little while, but he maintained something called the Quantum Algorithms Zoo.

HPCwire: Let's get back to the NIST effort to develop quantum-resistant algorithms. As I understand it, the process began being around 2016 has gone through this iterative process where you invite submissions of potential quantum resistant algorithms from the community, then test them and come up with some selections; there have been three rounds completed and in the process of becoming standards, with an ongoing fourth round. Walk me through the project and progress.

Dustin Moody: So these kinds of cryptographic competitions have been done in the past to select some of the algorithms that we use today. [So far] a widely used block cypher was selected through a competition. More recently a hash function. Back in 2016, we decided to do one of these [competitions] for new post quantum algorithms that we needed standards for. We let the community know about that. They're all excited and we got 82 submissions of which 69 met kind of the requirements that we'd set out to be

involved. Then we had a process that over six or seven years [during which] we evaluated them going through a period of rounds. In each round, we went further down to the most promising to advance the tons of work going on in there, both internally at NIST, and by the cryptographic community, doing research and benchmarks and experiments and everything.

The third round had seven finalists and eight alternate concluded in July of 2022, where we announced items that we would be standardizing as a result, that included one encryption algorithm and three signature algorithms. We did also keep a few encryption algorithms on into a fourth round for further study. They weren't quite ready to be selected for standardization. That fourth round is still ongoing and will probably end as this fall, and we'll pick one or two of those to also standardize. We'll have two or three encryption [methods] and three signatures as well.

HPCwire: It sounds like a relatively smooth process?

Dustin Moody: That process got a lot of attention from the community. A lot of the algorithms ended up being broken, some late in the process — that's kind of the nature of how this thing works. That's where we are now. We're just about done writing the standards for the first ones that we selected, our expected date is publishing them this summer. The fourth round will end this fall, and then we'll write standards for those that will take another year or two.

We also have ongoing work to select a few more digital signature algorithms as well. The reason for that is so many of the algorithms we selected are based on what are called lattices; they're the most promising family, [with] good performance, good security. And for signatures, we had two based on lattices, and then one not based on lattices. The one that wasn't based on lattices — it's called SPHINCS+ — turns out to be bigger and slower. So if applications needed to use it, it might not be ideal for them. We wanted to have a backup not based on lattices that could get used easily. That's what this ongoing digital signature process is about [and] we're encouraging researchers to try and design new solutions that are not based on lattices that are better performing.

HPCwire: When NIST assesses these algorithms, it must look to see how many computational resources are required to run them?

Dustin Moody: There's specific evaluation criteria that we look at. Number one is security. Number two is performance. And number three is this laundry list of everything else. But we work internally at NIST, we have a team of experts and try to work with cryptography and industry experts around the world who are independently doing it. But sometimes we're doing joint research with them in the field.

Security has a wide number of ways to look at it. There's the theoretical security, where you're trying to create security proofs where you're trying to say, 'if you can break my crypto system, then you can break this hard mathematical problem.' And we can give a proof for that and because that hard mathematical problem has been studied, that gives us a little bit more confidence. Then it gets complicated because we're used to doing this with classical computers and looking at how they can attack things. But now we have to look at how can quantum computers attack things and they don't yet exist. We don't know their performance. capabilities. So we have to extrapolate and do the best that we can. But it's all thrown into the mix.

Typically, you don't end up needing supercomputers. You're able to analyze how long would the attacks take, how many resources they take, if you were to fully tried to break the security parameters at current levels. The parameters are chosen so that it's [practically] infeasible to do so. You can figure out, if I were to break this, it would take, you know, 100 years, so there's no use in actually trying to do that unless you kind of find a breakthrough to find a different way. (See descriptive list of NIST strengths categories at end of article)

HPCwire: Do you test on today's NISQ (near-term intermediate scale quantum) computers?

Dustin Moody: They're too small right now to really have any impact in looking at how will a larger quantum computer fare against concrete parameters chosen at high enough security levels. So it's more theoretical, when you're figuring out how much resources it would take.

HPCwire: So summarizing a little bit, you think in the fall you'll finish this last fourth round. Those would all be candidates for standards, which then anyone could use for incorporation into encryption schemes that would be quantum computer resistant.

Dustin Moody: That's correct. The main ones that we expect to use were already selected in our first batch. So those are kind of the primary ones, most people will use those. But we need to have some backups in case you know, someone comes up with a new breakthrough.

HPCwire: When you select them do you deliberately have a range in terms of computational requirements, knowing that not everyone is going to have supercomputers at their doorstep. Many organizations may need to use more modest resources when running these encryption codes. So people could pick and choose a little bit based on the computational requirements.

Dustin Moody: Yes, there's a range of security categories from one to five. Category Five has the highest security, but performance is impacted. So there's a trade off. We include parameters for categories one, three, a five so people can choose the one that's best suited for their needs.

HPCwire: Can you talk a little bit about the Migration to PQC project, which is also I believe in NIST initiative to develop a variety of tools for implementingPQC What's your involvement? How is that going?

Dustin Moody: That project is being run by NIST's National Cybersecurity Center of Excellence (NCCoE). I'm not one of the managers but I attend all the meetings and I'm there to support what goes on. They've collaborated with…I think the list is up 40 or 50 industry partners and the list is on their website. It's a really strong collaboration. A lot of these companies on their own would typically be competing with each but here, they're all working for the common good of making the migration as smooth as possible, getting experience developing tools that people are going to need to do cryptographic inventories. That's kind of one of the first steps that an organization is going to need to do. Trying to make sure everything will be interoperable. What lessons can we learn as we. Some people are further along than others and how can we share that information best? It's really good to have weekly calls, [and] we hold events from time to time. Mostly these industry collaborators are driving it and talking with each other and we just kind of organize them together and help them to keep moving.

HPCwire: Is there any effort to build best practices in this area? Something that that NIST and these collaborators from industry and academia and DOE and DOD could all provide? It would be perhaps have the NIST stamp of authority on best practices for implementing quantum resistant cryptography.

Dustin Moody: Well, the standards that my team is writing, and those are written by NIST and those are the algorithms that people will implement. Then they'll also then get tested and validated by some of our labs at NIST. The migration project is producing documents, in a series (NIST SP 1800-38A, NIST SP 1800-38B, NIST SP 1800-38C) and those are updated from time to time, where they're sharing what they've learned and putting best practice in this. They are NIST documents, written jointly with the NIST team and with these collaborators to share what they've got so far.

HPCwire: What can the potential user community do to be involved? I realize the project is quite mature, it's been around for a while, and you've got lots of people who who've been involved already. Are we at the stage where the main participants are working with each other and NIST in

developing these algorithms, and it's now a matter of sort of monitoring the tools that come out.

Dustin Moody: I would say every organization should be becoming educated on understanding the quantum threat, knowing what's going on with standardization, knowing that you're going to need to migrate, and what that's going to involve your organization. It's not going to be easy and pain free. So planning ahead, and all that. If they want to join that that collaboration (Migration to PQC), people are still joining from time to time and it is still open if they have something that they've got to share. But for most organizations or groups, it's going to be just trying to create your plan preparing for the migration. We want you to wait till the final standards are published, so you're not implementing the something that's 99% the final standard, we want you to wait until that's there, but you can prepare now.

HPCwire: When will they be final?

Dustin Moody: Of the four that we selected, three of them. We put out draft standards a year ago, got public feedback, and have been revising since. The final versions are going to be published this summer. We don't have an exact date, but it will, it'll be this summer.

HPCwire: At that point, will a variety of requirements will come around using these algorithms, for example in the U.S. government and perhaps in industry requiring compliance?

Dustin Moody: Technically NIST isn't a regulatory agency. So yes, US government can. I think the OMB says that all agencies need to use our standards. So the federal government has to use the standards that we use for cryptography, but we know that a wider audience industry in the United States and globally tends to use the algorithms that we standardized as well.

HPCwire: We're in a world in which geopolitical tensions are real. Are we worried about rivals from China or Russia, or other competing nations not sharing their advances? Or is the cryptoanalyst community small enough that those kinds of things are not likely to happen because the people know each other?

Dustin Moody: There is a real geopolitical threat in terms of who gets the quantum computer quickest. If China develops that and they're able to break into our cryptography, that's a that's a real threat. In terms of designing the algorithms and making the standards, it's been a very cooperative effort internationally. Industry benefits when a lot of people are using the same algorithms all over the world. And we've seen other countries in global standards organizations say they're going to use the algorithms that were involved in our process.

There are some exceptions like China never trusting the United States. They're developing their own PQC standards. They're actually very, very similar to the algorithms [we're using] but they were selected internally. Russia has been doing their own thing, they don't really communicate with the rest of the world very much. I don't have a lot of information on what they're doing. China, even though they are doing their own standards, did have researchers participate in the process; they hosted one of the workshops in the field a few years back. So the community is small enough that people are very good at working together, even if sometimes the country will develop their own standards.

HPCwire: How did you get involved in cryptography? What drew you into this field?

Dustin Moody: Well, I love math and the math I was studying has some applications in cryptography, specifically, something called elliptic curves, and there's crypto systems we use today that are based on the curve, which is this beautiful mathematical object that probably no one ever thought they would be of any use in the in the real world. But it turns out they are for cryptography. So that's kind of my hook into cryptography.

I ended up at NIST because NIST has elliptic curve cryptography standards. I didn't know anything about post quantum cryptography. Around 2014, my boss said, we're going to put you in this project dealing with post quantum cryptography and I was like, 'What's this? I've no idea what this is.' Within a couple of years, it kind of really took off and grew and has become this high priority for the United States government. It's been a kind of a fun journey to be on.

HPCwire: Will the PQC project just continue or will it wrap up at some point?

Dustin Moody: We'll continue for a number of years. We still have the fourth round to finish. We're still doing this additional digital signature process, which will take several more years. But then again, every everything we do in the future needs to protect against quantum computers. So these initial standards will get published, they'll be done at some point, but all future cryptography standards will have to take the quantum threat into account. So it's kind of built in that we have to keep going for the future.

HPCwire: When you talk to the vendor community, they all say, "Encryption has been implemented in such a haphazard way across systems that it's everywhere, and that in simply finding where it exists in all those things is difficult." The real goal, they argue, should be to move to a more modular predictable approach. Is there a way NIST can influence that? Or the selection of the algorithms can influence that?

Dustin Moody: Yes, and no. It's very tricky. That idea you're talking about, sometimes the word cryptoagility gets thrown out there in that direction. A lot of people are talking about, okay, we're going to need to migrate these algorithms, this is an opportunity to redesign systems and protocols, maybe we can do it a little bit more intelligently than we did in the past. At the same time, it's difficult to do that, because you've got so many interconnected pieces doing so many things. So it's tricky to do, but we are encouraging people and having lots of conversations like with the migration and PQC project. We're encouraging people to think about this, to redesign systems and protocols when you're designing your applications. Knowing I need to transition to these algorithms, maybe I can redesign my system so that if I need to upgrade again, at some point, it'll be much easier to do. I can keep track of where my cryptography is, what happens when I'm using it, what information and protecting. I hope that we'll get some benefit out of this migration, but it's, it's certainly going to be very difficult, complicated and painful as well.

HPCwire: Do you have an off the top of your head checklist sort of five things you should be thinking about now to prepare for post quantum cryptography?

Dustin Moody: I'd say number one, just know that the migration is coming. The United States government is mandating their agencies to it, but industry as well as going to need to be doing this migration. The migration is not going to be easy, it's not going to be pain free. You should be educating yourself as to what PQC is, the whole quantum threat, and starting to figure out, where are you using cryptography, what information is protected with cryptography. As you noted, that's not as easy as it should be. "Very often, you're going to need to use sophisticated tools that are being developed to assist with that. Also talk to your vendors, your CIOs, your CEOs to make sure they're aware and that they're planning for budgets to do this. Just because a quantum computer [able to decrypt] isn't going to be built for, who knows, maybe 15 years, they may think I can just put this off, but understanding that threat is coming sooner than than you realize is important."

HPCwire: Thank you for your time!

34.What is post-quantum encryption?

Everything to know about the high-tech security feature adopted by Apple, Meta, and Zoom

by Michael Grothaus
https://www.fastcompany.com/91132623/post-quantum-encryption-what-is-apple-meta-zoom-signal-hdnl

Late last month, Zoom announced that it was rolling out a new type of encryption, called post-quantum cryptography (PQC), to its Zoom Workplace product. A day later, Facebook owner Meta revealed it had deployed post-quantum cryptography across most of its internal service communications. These announcements from the communications and social media giants came several months after Apple's February reveal that its iMessage platform would be the first major messaging platform to roll out the most advanced version of post-quantum cryptography to date, PQ3.

But PQC, PQ3, post-quantum cryptography—just what do all these terms mean? Here's what you need to know about post-quantum encryption and why it will be critical in protecting our most sensitive data in the decades ahead.

WHAT IS ENCRYPTION?

Before we can talk about post-quantum encryption, we need to talk about basic encryption.

Encryption is a term that most of us are familiar with. Encryption uses incredibly complex mathematical equations to scramble our data into an unreadable mess—our messages, documents, and photos—so that no one without the password- or PIN-protected encryption key can unscramble and read or view our data.

Today, there are two main types of encryption: regular encryption and end-to-end encryption (E2EE). If your data is merely encrypted—such as your DMs in the TikTok app—the sender, receiver, and messaging platform itself hold the keys to unencrypt and read your data. But if your data is end-to-end encrypted, only the sender and the receiver can read the data because only they hold the keys—not the messaging platform.

Any time you lock most devices, including laptops or smartphones, the data on them is usually encrypted and remains that way until the owner unlocks the device by authenticating themself with their biometrics, PIN, or password. And when it comes to communications, most major messaging platforms today, such as Apple's iMessage, Meta's WhatsApp, and Signal, are end-to-end encrypted.

Without the key to the encrypted data, gaining access to it is nearly impossible. Nearly. Since encryption is just a really complex equation, theoretically it can be broken by a powerful enough computer, given enough time. But even for today's most advanced supercomputers, breaking our current encryption technology would take millions or even *billions* of years.

The thing is, today's supercomputers are based on classical physics. The computers of tomorrow will be based on quantum physics—and quantum computers may be able to break our current encryption protections not in eons, but in seconds.

QUANTUM VERSUS CLASSICAL COMPUTERS

Any computer you've ever used is a classical computer. This is true no matter if it's a Commodore 64 from the 1980s, an M3 MacBook Pro from 2023, or the iPhone or Android in your pocket. These computers are called classical computers because they work on the principles of classical physics.

Quantum computers, on the other hand, are based on the mechanics and principles of quantum physics—and this gives them two big advantages—speed and power. Whereas a classical computer uses bits, with each bit being either a 1 or a 0, a quantum computer uses qubits (quantum bits). And because qubits can take advantage of quantum mechanics' strange superimposition properties, a qubit can be a 1 and a 0 *at the same time*. This duality makes quantum computers exponentially more powerful and faster than any classical computer in existence.

It also means a quantum computer could likely solve the encryption equation currently protecting your most sensitive health, financial, and personal data in no time at all—making today's classical encryption practically worthless in the years ahead.

ATTACKS FROM THE FUTURE

While quantum computers are likely to revolutionize specific fields including healthcare, finance, and various sciences, they also represent a threat to our data if weaponized by malicious nation-states or bad actors to break the encryption that keeps our data safe.

The good news is that today's quantum computers aren't advanced enough to break our current classical encryption. The bad news is that bad actors can already prepare for the day when they can use quantum computers against our data through what is known as "harvest now, decrypt later" (HNDL) attacks.

In an HNDL attack, a threat actor scoops up our encrypted data even though they can't crack it. However, they'll hold on to our unreadable data until a future date when a quantum computer can do the job. Experts disagree about when quantum computers will be powerful enough to unscramble our classically encrypted data, but many believe the threshold could happen in as few as five to ten years, with the most conservative estimates being about 30 years from now.

Of course, you may say, "Who cares if some hacker can read my data 30 years from now?" But the threat HNDL attacks pose depends on the type of data and the person whose data has been harvested. For example, your social security number will be just as valuable to a hacker thirty years from now as it is today. And if you're a journalist or activist operating in oppressive countries, your communications can put you or your contacts in danger no matter when that data is decrypted.

The threat of quantum computers and HNDL attacks are why companies such as Apple, the Signal Foundation, Meta, and Zoom have begun rolling out a new, advanced type of encryption: post-quantum encryption.

SO, WHAT IS POST-QUANTUM ENCRYPTION?

Post-quantum encryption, also called post-quantum cryptography (PQC), is a new type of encryption designed to be used today to protect our data from quantum computer attacks in the future.

Post-quantum encryption uses complex mathematics that makes it exponentially harder for tomorrow's quantum computers to break into our data. The hope is that post-quantum encryption applied to our data today will negate HNDL attacks since even if our data is harvested by bad actors today, they still

won't be able to decrypt it with quantum computers in 10 years or 30.

The Signal Foundation gets the credit for being the first major messaging app to roll out any type of post-quantum encryption, back in 2023—a type called PQXDH. Apple followed with post-quantum encryption in iMessage earlier this year, but a more advanced form it designated as "PQ3" (Signal's implementation would be classified as "PQ2" under this system—a less advanced version of PQC).

The bad thing about PQC is that the encryption technology is still relatively new, so there could be flaws in its design that quantum computers could exploit in the future. Also, current post-quantum encryption isn't standardized, so every company is doing its own thing at the moment—but that should change later this year when the National Institute of Standards and Technology (NIST) finalizes its PQC standard specifications.

In short, understand this: post-quantum encryption is the next phase in data encryption. If your app or device offers it today, you may not think it's a big deal. But thirty years from now, your data might thank you.