Crypto News

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

June 01, 2023

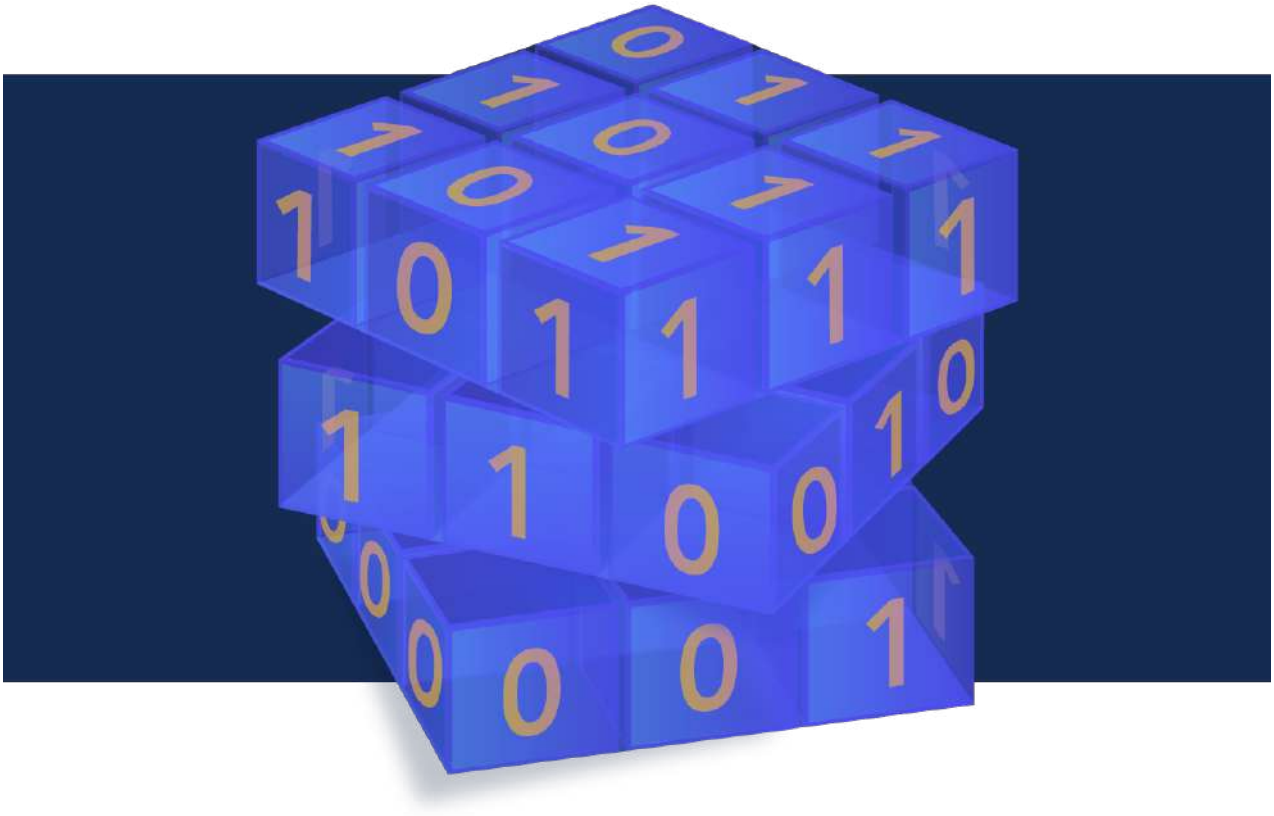


TABLE OF CONTENTS

Editorial

With it officially getting hotter out there, take a break with this month's newsletter by the pool to cool off. Let's get to it!

If you stay in the know about Quantum computing then you're well aware of IBMs market share in this space. Their continued influence is noted in article 2 which outlines their plans to build a 100,000 qubit computer over the next 10 years. They will partner with the University of Chicago and the University of Tokyo to make this $100 million project a reality. Just last year IBM created the largest quantum computing system with 433 qubits. Though this exponential increase in qubits seems astronomical and somewhat aspirational, the time frame to do the work seems realistic. What do you think? Do you think they can do it?

If you live in the United States, you'll be interested in article 19 which summarizes the US Governments release of the National Standards and Strategy for Critical and Emerging Technology. This strategy focuses on the US government's determination in protecting the technology that American's use regularly as well as their resolve in remaining not just competitive but the leaders in the development of international standards. The current US Presidential administration then takes cybersecurity to the private sector in article 25. In the recently released National Cyber Strategy, the administration would like a new social contract to be adopted by the private sector which would take the onus of cybersecurity off of individual users and put it back in the hands of the private sector. The basis for this is the idea that the private sector is the only group who can embed the "…security-first product development to protect the country's information architecture from the converging threats of the modernizing internet, quantum computing, and the hyper-connected Internet of Things (IoT)…" Though I agree with the overall idea that certain organizations and technologies need to have a larger cybersecurity focus, it's not feasible for all organizations and technologies. Those highlighted in the statement above are fair and should be putting the right guard rails in place to ensure their products are secure from the start and are continually upgraded to keep up with new and emerging threats. Make sure to make your way down to the end of the newsletter to get more details from this article.

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

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.Enterprise 'woefully unprepared' for quantum computing risk

by Ryan Morrison
https://techmonitor.ai/hardware/quantum/quantum-risk-computing-algorithm

Companies are 'woefully unprepared' for both the risks from and impact of quantum computing, warns ratings agency Moody's. This includes updating systems to use post-quantum cybersecurity. One analyst told *Tech Monitor* large organisations should have "readied themselves" by now for the impact the technology will have.

In its new quantum research report, Moody's spoke to 200 data, analytics and innovation leaders for financial services and banking companies across Europe and North America. It found 87% of companies lack the budget to adequately invest in the nascent technology.

The report also found that despite warnings from governments and cybersecurity professionals that quantum computers will be able to crack encryption, 86% of those companies surveyed admitted they are not ready for post-quantum cybersecurity. That is despite 84% saying they foresee the need to be ready in the next 2-5 years.

One of the biggest threats facing companies today is from hack now, decrypt later. This is the practice of cybercriminals stealing encrypted information with the intention of cracking it once quantum computers are powerful enough to break the encryption. Thanks to a better understanding of error mitigation and improved algorithms it is expected this point could be reached within a decade.

"Our survey revealed the top five high-potential use cases for quantum computing are: risk analysis, stress testing, cybersecurity, synthetic data, and the detection of fraud and money laundering," the authors explained. It could also power breakthroughs in high-frequency trading, fraud prevention and derivative pricing. All areas with complex calculations at the root.

The financial services sector is seen as an early adopter of the technology, with even today's noisy quantum hardware able to make an impact on areas like fraud detection and solving optimisation problems. The majority of the companies investigating quantum computing felt that risk analysis has the biggest potential for impacting the financial services sector. This is the process of identification, analysis and acceptance or mitigation of investment decisions. It contains a significant number of variables and points of consideration which is well suited to the way quantum hardware works.

A paper published in the journal Quantum Information Processing by Sascha Wilkens and Joe Moorhouse at BNP Paribas found that while the current number of available qubits is "far too low to render an actual business application viable" the constraint could be eased in the not too distant future with the advent of the first 1,000+ qubit machines. However, they explained that the million plus fault-tolerant qubit mark "certain computationally intensive algorithms and applications from the financial engineering world might be routinely handled with quantum hardware".

Too late to 'wait and see' on quantum computing

Sergio Gago, managing director for quantum computing at Moody's Analytics said: "While a 'wait and see strategy' is unsurprising, the rising tides of cyber and quantum risk necessitate action from the finance industry. The industry is unprepared for a 'Y2Q' event and there is a critical need for education

both at the executive and technical levels."

He warned that every financial institution should have a quantum cybersecurity strategy in place today. If that 86% unpreparedness rate is reflective of enterprise as a whole then it would be a "concerning metric" particularly for financial institutions.

Preparing for a post-quantum cybersecurity environment will require more than just switching to a post-quantum form of cryptography. Many of the existing encryption systems are "on chip" or built into a device. There are also risks throughout the supply chain with significant changes to infrastructure required.

Writing in the report for Moody's Julian van Velzen, CTIO and head of Capgemini's Quantum Lab, emphasised the importance of post-quantum cryptography, particularly in the financial sector. "The thing about post-quantum cryptography is that it's essential for everyone who has critical infrastructure, such as utilities and financial services," he said. "It's crucial to have secure encryption methods to protect our customers' information."

Overall, only 14% of respondents are actively developing quantum computing capabilities either in-house or with external partners. Kristin M. Gilkes, EY Global Innovation's quantum leader said any large company not actively exploring quantum needs to take action. Speaking to *Tech Monitor* prior to the Moody's report's publication, Gilkes said "it isn't too late" for businesses to get up to speed on quantum risk.

"I don't think that it requires a lot of investment," Gilkes said. "We're really trying to democratize this in such a way that everybody can experiment with it. I think that companies should think of it from an offence and defence perspective. If they're limited or constrained, then perhaps they should really consider the defensive side, which would be the cyber security side, quantum encryption, end to end, that sort of thing."

2.IBM wants to build a 100,000-qubit quantum computer

by Michael Brooks

https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/

Late last year, IBM took the record for the largest quantum computing system with a processor that contained 433 quantum bits, or qubits, the fundamental building blocks of quantum information processing. Now, the company has set its sights on a much bigger target: a 100,000-qubit machine that it aims to build within 10 years.

IBM made the announcement on May 22 at the G7 summit in Hiroshima, Japan. The company will partner with the University of Tokyo and the University of Chicago in a $100 million dollar initiative to push quantum computing into the realm of full-scale operation, where the technology could potentially tackle pressing problems that no standard supercomputer can solve.

Or at least it can't solve them alone. The idea is that the 100,000 qubits will work alongside the best "classical" supercomputers to achieve new breakthroughs in drug discovery, fertilizer production, battery performance, and a host of other applications. "I call this quantum-centric supercomputing," IBM's VP of quantum, Jay Gambetta, told MIT Technology Review in an in-person interview in London last week.

Quantum computing holds and processes information in a way that exploits the unique properties of fundamental particles: electrons, atoms, and small molecules can exist in multiple energy states at once, a phenomenon known as superposition, and the states of particles can become linked, or entangled, with one another. This means that information can be encoded and manipulated in novel ways, opening the door to a swath of classically impossible computing tasks.

As yet, quantum computers have not achieved anything useful that standard supercomputers cannot do. That is largely because they haven't had enough qubits and because the systems are easily disrupted by tiny perturbations in their environment that physicists call noise.

Researchers have been exploring ways to make do with noisy systems, but many expect that quantum systems will have to scale up significantly to be truly useful, so that they can devote a large fraction of their qubits to correcting the errors induced by noise.

IBM is not the first to aim big. Google has said it is targeting a million qubits by the end of the decade, though error correction means only 10,000 will be available for computations. Maryland-based IonQ is aiming to have 1,024 "logical qubits," each of which will be formed from an error-correcting circuit of 13 physical qubits, performing computations by 2028. Palo Alto–based PsiQuantum, like Google, is also aiming to build a million-qubit quantum computer, but it has not revealed its time scale or its error-correction requirements.

Because of those requirements, citing the number of physical qubits is something of a red herring—the particulars of how they are built, which affect factors such as their resilience to noise and their ease of operation, are crucially important. The companies involved usually offer additional measures of performance, such as "quantum volume" and the number of "algorithmic qubits." In the next decade advances in error correction, qubit performance, and software-led error "mitigation," as well as the major distinctions between different types of qubits, will make this race especially tricky to follow.

Refining the hardware

IBM's qubits are currently made from rings of superconducting metal, which follow the same rules as atoms when operated at millikelvin temperatures, just a tiny fraction of a degree above absolute zero. In theory, these qubits can be operated in a large ensemble. But according to IBM's own road map, quantum computers of the sort it's building can only scale up to 5,000 qubits with current technology. Most experts say that's not big enough to yield much in the way of useful computation. To create powerful quantum computers, engineers will have to go bigger. And that will require new technology.

One example of what's needed is much more energy-efficient control of qubits. At the moment, each one of IBM's superconducting qubits requires around 65 watts to operate. "If I want to do 100,000, that's a lot of energy: I'm going to need something the size of a building, and a nuclear power plant and a billion dollars, to make one machine," Gambetta says. "That's obviously ludicrous. To get from 5,000 to 100,000, we clearly need innovation."

IBM has already done proof-of-principle experiments showing that integrated circuits based on "complementary metal oxide semiconductor" (CMOS) technology can be installed next to the cold qubits to control them with just tens of milliwatts. Beyond that, he admits, the technology required for quantum-centric supercomputing does not yet exist: that is why academic research is a vital part of the project.

The qubits will exist on a type of modular chip that is only just beginning to take shape in IBM labs. Modularity, essential when it will be impossible to put enough qubits on a single chip, requires interconnects that transfer quantum information between modules. IBM's "Kookaburra," a 1,386-qubit multichip processor with a quantum communication link, is under development and slated for release in 2025.

Other necessary innovations are where the universities come in. Researchers at Tokyo and Chicago have already made significant strides in areas such as components and communication innovations that could be vital parts of the final product, Gambetta says. He thinks there will likely be many more industry-academic collaborations to come over the next decade. “We have to help the universities do what they do best,” he says. Google is of the same mind: in a separate deal, it is devoting $50 million to funding for quantum computing research in the same two universities.

Gambetta says the industry also needs more “quantum computational scientists,” people skilled in bridging the divide between the physicists creating the machine and the developers looking to design and implement useful algorithms.

Software that runs on quantum machines will be vitally important too. “We want to create the industry as fast as possible, and the best way to do that is to get people developing the equivalent of our classical software libraries,” Gambetta says. It’s why IBM has worked to make its systems available to academic researchers over the last few years, he says: IBM’s quantum processors can be put to work via the cloud using custom-built interfaces that require minimal understanding of the technicalities of quantum computing. He says there have been some 2,000 research papers written about experiments using the company’s quantum devices: “To me that’s a good indication of innovation happening.”

There is no guarantee that the $100 million earmarked for this project will be enough to achieve the 100,000-qubit goal. “There’s definitely risk,” Gambetta says.

Joe Fitzsimons, CEO of Horizon Quantum, a Singapore-based quantum software developer, agrees. “This is unlikely to be a completely smooth journey without surprises,” he says.

But, he adds, it’s a risk that has to be taken: the industry has to face the fear of failure and make attempts to overcome the technical challenges facing large-scale quantum computing. IBM’s plan seems reasonable, Fitzsimons says, although there are plenty of potential roadblocks. “At this scale, control systems will be a limiting factor and will need to evolve significantly to support such a large number of qubits in a reasonably efficient way,” he says.

3.How Europe Can Become a Leader in Quantum Technology

by Michele Canzi

https://quantumcomputingreport.com/how-europe-can-become-a-leader-in-quantum-technology/

Depending on who you ask, quantum computers are going to solve *almost* all of mankind’s problems. Everything, from the financial markets to medicine, is going to be flipped on its head – because quantum computers will be to classical computers what the Falcon 9 is to a bicycle. The field is moving fast, and Quantum Supremacy – the stage where a quantum device can solve a problem that no classical computer can solve in any feasible amount of time – is almost in the rear-view mirror.

Once they’ll get there, quantum computers will transform everything. But for now, there aren’t just that many people who know how to build them. These chandelier-looking machines are quasi-hand-built by PhDs in physics. And at the moment, the industry roadmap has at least one glaring pothole: a lack of trained people.

In deep learning, fewer than 25,000 people can be considered world experts. The labor pool in quantum computing is significantly smaller. By some accounts, fewer than a thousand people in the world are doing leading research in the field. Scientists who build these systems specialize in quantum physics, which focuses on the unique behavior of matter and energy at their most fundamental level—atomic and subatomic scales. This involves studying the very small, very isolated, or very cold, which is nothing like the physics we experience in our day-to-day lives.

The crux of the matter extends beyond the industry shortage of quantum skills. There are also academic obstacles. While you might not need to be a quantum physicist to get hired by a quantum tech startup, the theory behind quantum computing is so deeply intertwined with elements of quantum physics, advanced math, and a wealth of interdisciplinary skills, a Ph.D.-level knowledge is almost necessary. Today, there are simply not enough profiles who understand what goes on "under the hood" of a quantum computer.

Europe's rich history in mathematics and physics has laid the foundation for today's quantum computing industry. At the dawn of the 20th century, Newton's laws of motion and Maxwell's laws of light and electromagnetism could explain the entire physical. Einstein, who used Planck's theory to explain the photoelectric effect, and Schrödinger, with his fundamental wave equation, revolutionized the field. Bohr contributed the particle-wave concept, while Heisenberg introduced the uncertainty principle. A legacy of scientific trailblazers laid the foundations for the next technological paradigm.

This robust academic fabric allowed Europe to accumulate a wealth of publications. While the US has produced more impactful articles, Europe takes the lead in the volume of quantum-related publications and outperforms American institutions (McKinsey Quantum Technology Monitor, April 2023, page 46). This comes as no surprise, given that the quantum tech talent pool in Europe is not only more than twice the size of that in the US but also nearly three times denser (McKinsey Quantum Technology Monitor, April 2023, page 48).

Dr. Jan Goetz, CEO and co-founder of IQM Quantum Computers, identifies Europe's strong research sector as a magnet for investors. According to Goetz, Europe's strengths lie in its scientific research, which is integral to quantum breakthroughs. "This is a very big chance for Europe because the money typically goes to where the good people are," Goetz said. "And as this field is now emerging from the academic sector into the commercial sector, the money goes to the best research teams in the world. And Europe really has the world's leading research teams."

But Europe's advantage in quantum tech is not only limited to highly specialized talent. The European Union has made billions of euros available for developing quantum technologies, especially for quantum computing. Germany alone has committed €2.2 billion, while the EU has committed more than €145 billion over the next two to three years to develop next-generation processors, with some of that investment dedicated to quantum.

Europe also dominates in the key industry verticals that will benefit the most from the exponentially faster computation that quantum computers will enable – especially in material science, chemistry, and pharmaceuticals. In a way, the key industry verticals that would benefit the most from the quantum revolution are already well-established in Europe. The customer ecosystem is already there.

Of course, this analysis should include lots of caveats. Building a regional industrial ecosystem is not just a matter of talent pool It requires substantial public sector involvement, efficient capital markets, and attractive salaries, just to begin with. But all of these elements are not interchangeable. Highly skilled human capital is orders of magnitude more valuable than financial capital. And its value only increases over time, as we get closer to the quantum revolution.

That kind of specialized, ultra-rare talent is the fuel of all transformative technological revolutions. The history of technological progress is predicated on the ability of geographical ecosystems to play

the *right* game with a *large enough* number of shots on goal. More quantum technologists, more shots on goal.

What the top 1% of most talented and ambitious people choose to do with their one and precious life has a dramatic impact on their environment. In medieval Europe, literacy was the great "technology of ambition" – if you could write down instructions and there were people who could read them, you could administrate at scale. By the late 18th century, armies were professionalizing and the modern state was emerging. The military command was the new 'technology of ambition'. Skip another couple of generations and finance emerges as the dominant 'technology of ambition'. Cheques and memos written in London reverberate around the world.

Ambitious people have gone from writing cheques to writing software – and, in the future, quantum software. By the numbers, Europe has more shots on goal to capitalize on the next "technology of ambition" and transform everything from warfare cybersecurity to drug discovery – and a thousand other things in between that we now take for granted. Europe's quantum legacy is a crescendo a century in the making.

4.How does Post-Quantum Cryptography affect the TLS protocol?

by Kimmo Jarvinen
https://www.design-reuse.com/industryexpertblogs/54083/how-does-post-quantum-cryptography-affect-the-tls-protocol.html

The emerging threat of quantum computers changes the way we look at and implement communications security of today. How can Post-Quantum Cryptography (PQC) be used for protecting the widely used TLS 1.3 protocol?

Transport Layer Security (TLS) is perhaps the most well-known cryptographic protocol. It is used for providing communication in a large variety of applications security including secure web browsing. Typically, web browsers show a lock icon next to the URL link when it is using the protected HTTPS protocol; this means that the communication is protected with TLS. Although secure web browsing is the most visible application of TLS, it is nowadays used in a large variety of different applications including also machine-to-machine communication protocols.

The history of TLS dates back to the 1990s. It was developed by Netscape Communications and was originally called Secure Sockets Layer (SSL). TLS 1.0 was released as **RFC 2246** by the IETF (Internet Engineering Task Force) in 1999. The early version of both SSL and TLS suffered from severe vulnerabilities and they are no longer recommended to be used. Nowadays, basically two version of TLS are in mainstream use: TLS 1.2 defined in RFC 5246 from 2008 and **TLS 1.3** defined in **RFC 8446** from 2018. The latter includes significant security and performance improvements over the earlier versions and is the recommended version for any new systems.

TLS Handshake – how does it work?

TLS involves two parties: a client and a server. A TLS session is initiated by the client and it begins with a TLS Handshake. During the Handshake,

1. the client and server **agree upon the cryptographic algorithms** that are used in Handshake and the

communication;

2. the client and server **exchange a shared secret key** that later is used for protecting client-server communication;

3. the **client authenticates the server** by using the server's certificate; and

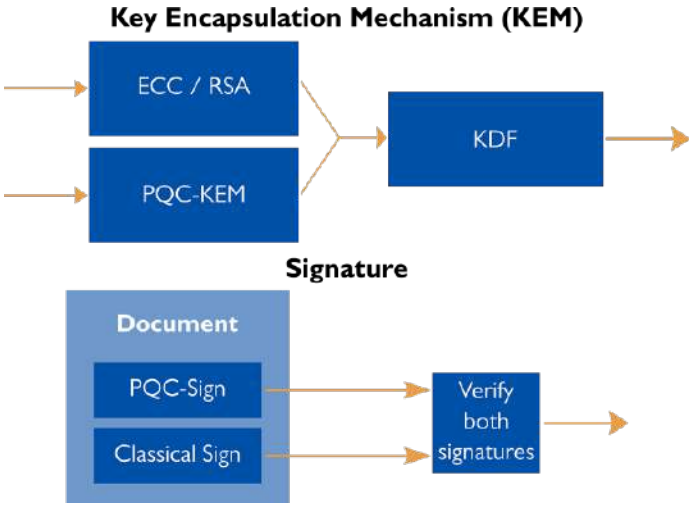
4. optionally the **server also authenticates the client** by using the client's certificate (however, it is more common that if client authentication is needed, then it is done with a separate protocol over the established TLS session);

When the TLS Handshake has been finished successfully, the main communication is protected for both confidentiality and authenticity/integrity by using the shared secret key. Most commonly the communication is nowadays protected using the AES-GCM authenticated encryption scheme, but other alternatives are also possible (for example, ChaCha20-Poly1305 or AES-CBC + HMAC).

New post-quantum winds

The most significant new thing in contemporary cryptography is the shift to Post-Quantum Cryptography (PQC). The traditional asymmetric (public key) cryptography methods RSA and Elliptic Curve Cryptography (ECC) are vulnerable to quantum attacks if large enough quantum computers become reality. PQC are algorithms that are not affected by the emerging quantum threat and are eventually to be used as replacements of the current RSA and ECC.

Various standardisation bodies and government authorities are currently setting standards and requirements for shifting to PQC in practical systems. Most importantly, the American NIST has been running a standardisation process for finding secure and efficient PQC algorithms for key exchange and digital signatures. In summer 2022, they concluded the selection process and announced four algorithms – one for key exchange and three for signatures – that are to be included in the first PQC standard. The key exchange algorithm is called CRYSTALS-Kyber and the primary signature algorithm is called CRYSTALS-Dilithium. Being new, PQC algorithms have not yet reached the same level of confidence in their security that, for example, RSA and ECC have. As a consequence, it is generally recommended not to directly replace the traditional algorithms with the new PQC algorithms but, instead, use a hybrid solution where the security relies on both ECC and PQC. In such a hybrid solution, PQC offers protection against future adversaries that may be able to leverage quantum computers in attacks, and ECC provides fallback security against possible, yet unlikely, failures of PQC algorithms under more traditional cryptanalytic attacks.



Enter Post-Quantum TLS

Both the key exchange and server (and client) authentication of TLS Handshake rely heavily on the use of asymmetric cryptography and, nowadays, especially on ECC. Thus, the security of the TLS Handshake as defined in TLS 1.2 or TLS 1.3 is affected by the quantum threat, and there must be a roadmap for adopting PQC algorithms in TLS.

Indeed, the work for Post-Quantum TLS (PQ-TLS) has already began: for example, Stebila (Univ. Waterloo), Fluhrer (Cisco), and Gueron (Amazon Web Services) have published an internet draft describing the use of hybrid key exchange in TLS 1.3. They describe a scheme for using two (or more) algorithms in TLS 1.3 key exchange in a way that the security of the TLS Handshake remains secure as long as one of the algorithms remains unbroken. A natural application for their scheme is to combine a PQC algorithm with ECC in order to implement an aforementioned hybrid solution. They propose four such combinations in their draft, where different elliptic curves are combined with CRYSTALS-Kyber. These combinations and their different key lengths are targeted for various use cases depending on their communication bandwidths and other requirements.

It is noteworthy that the above proposal is only for key exchange, and it does not propose anything for authentication (that is, digital signatures). The motivation for this is that the proposal suggests a protection method against future adversaries and assumes that quantum attacks are not possible today. Hence, TLS session needs to be protected against adversaries who record session communication so that they could later break the security with a quantum computer and find out what was being communicated. Such an adversary could break the confidentiality protection of the TLS session by finding out the shared secret key by breaking ECC with a quantum computer, but breaking authentication retrospectively would not help the adversary because the session would have been closed long time ago.

5.Intrinsic Id PUFs: An Antidote to Post-Quantum Uncertainty

by Intrinsic ID

https://www.design-reuse.com/articles/54065/intrinsic-id-pufs-an-antidote-to-post-quantum-uncertainty.html

You've probably been hearing a lot lately about the quantum-computing threat to cryptography. If so, you probably also have a lot of questions about what this "quantum threat" is and how it will impact your cryptographic solutions. Let's take a look at some of the most common questions about quantum computing and its impact on cryptography.

What is a quantum computer?

A quantum computer is not a very fast general-purpose supercomputer, nor can it magically operate in a massively parallel manner. Instead, it efficiently executes unique quantum algorithms. These algorithms can in theory perform certain very specific computations much more efficiently than any traditional computer could.

However, the development of a meaningful quantum computer, i.e., one that can in practice outperform a modern traditional computer, is exceptionally difficult. Quantum computing technology has been in development since the 1980s, with gradually improving operational quantum computers since the 2010s.

However, even extrapolating the current state of the art into the future, and assuming an exponential improvement equivalent to Moore's law for traditional computers, experts estimate[1] that it will still take at least 15 to 20 years for a meaningful quantum computer to become a reality[2].

What is the quantum threat to cryptography?

In the 1990s, it was discovered that some quantum algorithms can impact the security of certain traditional cryptographic techniques. **Two quantum algorithms have raised concern**:

1. **Shor's algorithm**, invented in 1994 by Peter Shor, is an efficient quantum algorithm for factoring large integers, and for solving a few related number-theoretical problems. Currently, there are no known efficient-factoring algorithms for traditional computers, a fact that provides the basis of security for several classic public-key cryptographic techniques.

2. **Grover's algorithm**, invented in 1996 by Lov Grover, is a quantum algorithm that can search for the inverse of a generic function quadratically faster than a traditional computer can. In cryptographic terms, searching for inverses is equivalent to a brute-force attack (e.g., on an unknown secret key value). The difficulty of such attacks forms the basis of security for most symmetric cryptography primitives.

These quantum algorithms, if they can be executed on a meaningful quantum computer, will impact the security of current cryptographic techniques.

What is the impact on my public-key cryptography solutions?

By far the most important and most widely used public-key primitives today are based on RSA, discrete-logarithm, or elliptic curve cryptography. When meaningful quantum computers become operational, all of these can be efficiently solved by Shor's algorithm. This will make virtually all public-key cryptography in current use insecure.

For the affected public-key encryption and key exchange primitives, this threat is already real today. An attacker capturing and storing encrypted messages exchanged now (or in the past), could decrypt them in the future when meaningful quantum computers are operational. So, highly sensitive and/or long-term secrets communicated up to today are already at risk.

If you use the affected signing primitives in short-term commitments of less than 15 years, the problem is less urgent. However, if meaningful quantum computers become available, the value of any signature will be voided from that point. So, you shouldn't use the affected primitives for signing long-term commitments that still need to be verifiable in 15-20 years or more.

Over the last decade, the cryptographic community has designed new public-key primitives that are based on mathematical problems that cannot be solved by Shor's algorithm (or any other known efficient algorithm, quantum or otherwise). These algorithms are generally referred to as postquantum cryptography. NIST recently announced a selection of these algorithms for standardization[3].

What is the impact on my symmetric cryptography solutions?

---

[1] "**Report on Post-Quantum Cryptography**", NIST Information Technology Laboratory, NISTIR 8105, April 2016,

[2] "**2021 Quantum Threat Timeline Report**", Global Risk Institute (GRI), M. Mosca and M. Piani, January, 2022,

[3] "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates", NIST Information Technology Laboratory, July 5, 2022,

The security level of a well-designed symmetric key primitive is equivalent to the effort needed for brute-forcing the secret key. On a traditional computer, the effort of brute-forcing a secret key is directly exponential in the key's length. When a meaningful quantum computer can be used, Grover's algorithm can speed up the brute-force attack quadratically. The needed effort remains exponential, though only in half of the key's length. So, Grover's algorithm could be said to reduce the security of any given-length algorithm by 50%.

However, there are some important things to keep in mind:

- Grover's algorithm is an optimal brute-force strategy (quantum or otherwise)[4], so the quadratic speed-up is the worst-case security impact.

- There are strong indications that it is not possible to meaningfully parallelize the execution of Grover's algorithm[5] [6] [7]. In a traditional brute-force attack, doubling the number of computers used will cut the computation time in half. Such a scaling is not possible for Grover's algorithm on a quantum computer, which makes its use in a brute-force attack very impractical.

- Before Grover's algorithm can be used to perform real-world brute-force attacks on 128-bit keys, the performance of quantum computers must improve tremendously. Very modern traditional supercomputers can barely perform computations with a complexity exponential in 128/2 = 64 bits in a practically feasible time (several months). Based on their current state and rate of progress, it will be much, much more than 20 years before quantum computers could be at that same level.

The practical impact of quantum computers on symmetric cryptography is, for the moment, very limited. Worst-case, the security strength of currently used primitives is reduced by 50% (of their key length), but due to the limitations of Grover's algorithm, that is an overly pessimistic assumption for the near future. Doubling the length of symmetric keys to withstand quantum brute-force attacks is a very broad blanket measure that will certainly solve the problem, but is too conservative. Today, there are no mandated recommendations for quantum-hardening symmetric-key cryptography, and 128-bit security strength primitives like AES-128 or SHA-256 are considered safe to use now and in the foreseeable future.

Is there an impact on information-theoretical security?

Information-theoretically secure methods (also called unconditional or perfect security) are algorithmic techniques for which security claims are mathematically proven. Some important information-theoretically secure constructions and primitives include the Vernam cipher, Shamir's secret sharing, Quantum key distribution[8] (not to be confused with post-quantum cryptography), entropy sources and physical unclonable functions (PUFs), and fuzzy commitment schemes[9].

---

[4] "Grover's quantum searching algorithm is optimal", C. Zalka, Phys. Rev. A 60, 2746, October 1, 1999, **https://journals.aps.org/pra/abstract/10.1103/PhysRevA.60.2746**

[5] "**Reassessing Grover's Algorithm**", S. Fluhrer, IACR ePrint 2017/811,

[6] "**NIST's pleasant post-quantum surprise**", Bas Westerbaan, CloudFlare, July 8, 2022,

[7] "Post-Quantum Cryptography - FAQs: To protect against the threat of quantum computers, should we double the key length for AES now? (added 11/18/18)", NIST Information Technology Laboratory,

[8] "**Quantum cryptography: Public key distribution and coin tossing**", C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, December, 1984,

[9] "**A fuzzy commitment scheme**", A. Juels and M. Wattenberg, Proceedings of the 6th ACM conference on Computer and Communications Security, November, 1999,

The practical impact of quantum computers on symmetric cryptography is, for the moment, very limited.

Because an information-theoretical proof demonstrates that an adversary does not have sufficient information to break the security claim, regardless of its computing power – quantum or otherwise – information-theoretically secure constructions are not impacted by the quantum threat.

Intrinsic ID PUFs: An antidote for post-quantum security uncertainty

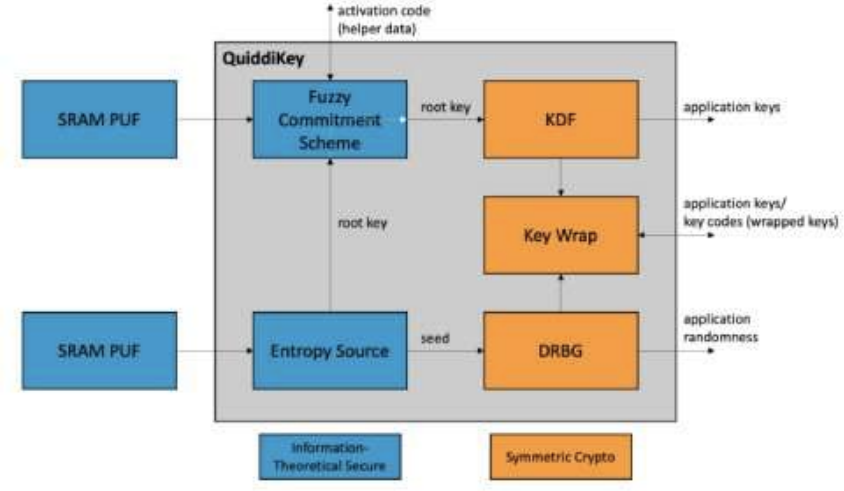
- **Intrinsic ID SRAM PUFs**

  The core technology underpinning all Intrinsic ID products is an SRAM PUF. Like other PUFs, an SRAM PUF generates device-unique responses that stem from unpredictable variations originating in the production process of silicon chips. The operation of an SRAM PUF is based on a conventional SRAM circuit readily available in virtually all digital chips.

  Based on years of continuous measurements and analysis, Intrinsic ID has developed stochastic models that describe the behavior of its SRAM PUFs very accurately[10]. Using these models, we can determine tight bounds on the unpredictability of SRAM PUFs. These unpredictability bounds are expressed in terms of entropy, and are fundamental in nature, and cannot be overcome by any amount of computation, quantum or otherwise.

- **Intrinsic ID Quiddikey**

  QuiddiKey is a hardware security solution based on SRAM PUF technology. The central component of QuiddiKey is a fuzzy commitment scheme that protects a root key with an SRAM PUF response and produces public helper data. It is information-theoretically proven that the helper data discloses zero information on the root key, so the fact that the helper data is public has no impact on the root key's security.



This no-leakage proof – kept intact over years of field deployment on hundreds of millions of devices – relies on the PUF employed by the system to be an entropy source, as expressed by its

[10] "An Accurate Probabilistic Reliability Model for Silicon PUFs", R. Maes, Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, 2013,

stochastic model. QuiddiKey uses its entropy source to initialize its root key for the very first time, which is subsequently protected by the fuzzy commitment scheme.

In addition to the fuzzy commitment scheme and the entropy source, QuiddiKey also implements cryptographic operations based on certified standard-compliant constructions making use of standard symmetric crypto primitives, particularly AES and SHA-256[11]. These operations include:

- a key derivation function (KDF) that uses the root key protected by the fuzzy commitment scheme as a key derivation key.
- a deterministic random bit generator (DRBG) that is initially seeded by a high-entropy seed coming from the entropy source.
- key wrapping functionality, essentially a form of authenticated encryption, for the protection of externally provided application keys using a key-wrapping key derived from the root key protected by the fuzzy commitment scheme.

- **Intrinsic ID: proven security for a post-quantum world**

The security architecture of QuiddiKey is based on information-theoretically secure components for the generation and protection of a root key, and on established symmetric cryptography for other cryptographic functions. Information-theoretically secure constructions are impervious to quantum attacks. The impact of the quantum threat on symmetric cryptography is very limited and does not require any remediation now or in the foreseeable future. Importantly, QuiddiKey does not deploy any quantum-vulnerable public-key cryptographic primitives.

All variants of QuiddiKey are quantum-secure and in accordance with recommended post-quantum guidelines. The use of the 256-bit security strength variant of QuiddiKey will offer strong quantumresistance, even in a distant future, but also the 128-bit variant is considered perfectly safe to use now and in the foreseeable time to come.

6.The State of Post Quantum Preparedness, from an Analyst Perspective

by Samantha Mabey
https://www.entrust.com/blog/2023/05/the-state-of-post-quantum-preparedness-from-an-analyst-perspective/

As part of my hosting duties on the Entrust Engage podcast, I've had the pleasure of speaking to some outstanding guests on a variety of topics from the science behind quantum computers themselves, to impacts post-quantum will have on digital security. In the latest episode, I was pleased to get a perspective I hadn't yet – that of an analyst – when I was joined by guest speaker, Forrester Principal Analyst Sandy Carielli. As we set up the discussion for the episode, here are some of the insights she provided on the state of post-quantum preparedness:

Samantha Mabey: Where do you currently feel like organizations are with looking at PQ and kicking off

[11] NIST Information Technology Laboratory, Cryptographic Algorithm Validation Program CAVP, validation #A2516, **https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=35127**

preparations to prepare against and mitigate the threat?

Sandy Carielli: Organizations are in the early stages of PQ preparation. The financial services and public sectors are the farthest ahead in this area, not surprising given the sensitivity of the data that traverses their systems. The Quantum Computing Cybersecurity Practices Act signed by President Biden at the end of last year speaks to the attention that government is placing on PQ, and the recently unveiled National Cybersecurity Strategy also stresses the importance of planning for the transition to post-quantum cryptography. However, even those industries paying close attention to PQ are at the early stages – aside from a few pilots and proofs of concept, organizations are primarily at the planning stage, with some kicking off cryptographic inventories.

SM: What do you foresee being some of the greatest challenges that organizations will face in preparing for the migration to post-quantum cyrptography?

SC: Cryptographic migration is never easy – previous migrations, such as from SHA-1 to SHA-256, have taken years. Even increasing the key size, such as moving from 1024 to 2048-bit RSA, doesn't happen overnight. The migration from RSA or ECC to a post-quantum algorithm will be even more complicated – given how deeply embedded cryptographic functions are in code and devices, rip and replace is rarely simple. For software and systems that organizations develop themselves, development teams will need to replace existing cryptographic code with new libraries, but standard implementations of the NIST selected algorithms aren't widespread. Then there's the supply chain issue – organizations will rely on their partners and vendors to update cryptographic implementations in their own products before the organization can fully migrate to PQ.

SM: While there is a consensus that the threat (of a quantum computer being able to break traditional public key cryptography in use today) is possibly a decade away, there is a more immediate threat known as "harvest now, decrypt later". Do you feel like there is a lack of awareness of this threat and that it further justifies that the need to prepare for PQ now?

SC: The "harvest now, decrypt later" threat is understood in pockets, such as government and financial services, and these are the areas where that threat is critical – customers' bank account numbers and citizens' government identification numbers are not likely to change in ten or twenty years. This is why these sectors have started to prepare and must continue to do so – they realize that they will need to have migrated to PQ long before a quantum computer is able to break traditional public key cryptography, and that attackers won't be able to decrypt any PQ-encrypted data that they harvest. Outside of that, security leaders are not as aware of the "harvest now, decrypt later" threat – leaders must realize that any harvested data protected with RSA or ECC could be vulnerable later, including account information, intellectual property, and personal information (which an attacker could use as blackmail material). Broader awareness of the "harvest now, decrypt later" threat would help organizations support PQ preparation strategies.

7.Quantum computers: coming to a data centre near you?

by Ryan Morrison
https://techmonitor.ai/hardware/quantum/data-centre-quantum-computer

Quantum software company QCWare is rolling out a hybrid platform with quantum emulators, quantum computer and classical supercomputers running together at a new data centre in Germany. It is the lat-

est in a line of similar projects looking to embed quantum machines in data centre infrastructure, but deployments remain at an early stage, industry insiders say.

Despite a number of high-profile announcements, including Equinix bringing a machine by Oxford Quantum Circuits into its Tokyo IBX Data Centre, and IBM expanding its Quantum Cloud, the quantum computing industry is still in its relative infancy.

Quantum computers are slowly increasing in performance, with higher numbers of qubits and greater coherence, but remain error-prone and noisy. This makes it harder to accurately process information. Fault-tolerant machines are on the horizon, and with new developments in topological qubits, as well as improved error corrections, some experts predict we will see quantum advantage, the point at which quantum machines can outperform their classical counterparts, within the next three to five years. Others are less optimistic, and suggest it could still be at least a decade away.

The most common types of quantum machines also require cooling to close to absolute zero, which makes them energy expensive. At a time when data centre owners are under increasing pressure to reduce energy usage, the demand has to be there to justify the expense of quantum hardware. And with many operating on low margins, they tend to err on the side of caution.

Data centre expert Paul Bevan, research director at Bloor Research, says for now quantum computers tend to be mainly found in supercomputing centres and national labs. He told *Tech Monitor* we are starting to see a gradual roll-out into mainstream data centres, particularly those belonging to the public cloud hyperscalers, but it is very early days.

This is because “the occupancy rates of co-location, wholesale and resale facilities are pretty good,” Bloor says. “There wasn’t the slowdown after Covid-19 many suspected, we didn’t see a massive reverse,” he explains. The rapid expansion of the cloud picked up some of the slack, and the rise of generative AI is adding further to demand for compute space.

He said that there is a long-lead time when it comes to investing in new leading-edge data centres and while they can be put up quickly, the planning and financing process can take up to a decade.

“Quantum is still very niche. Equinix are unusual, they are more forward-thinking than usual,” Bloor says. “Data centre owners and investors’ real focus is energy efficiency. They are being hit from all sides on the subject and so they are asking themselves ‘how I stop myself getting beaten up on energy use’. Couple that with the fact it is a low-margin business and you can see why there might be a reluctance to adopt a niche technology.”

How quantum computing will progress to the data centre

Quantum computing also goes against the principles of cloud computing, Bloor says. “In cloud you develop fast, fail forward, iterate and then iterate again,” he explains “We are nowhere near there with quantum. You have to engineer it to a point where it will work and right now there are still challenges to address to get it to run effectively on an ongoing basis to make it move beyond the lab.”

Data is likely to have the biggest impact on whether data centre owners take the plunge on installing costly quantum hardware. That is where companies like QCWare come into the picture, through hybrid and co-located solutions. It has partnered with QuiX Quantum to co-locate hardware onsite in a new data centre in the Netherlands that will integrate high-performance computing infrastructure with native quantum computing technology. It will be fully operational in August and the company says it will include shared memory access between the quantum and classical hardware.

This is an example of the benefits of having quantum and classical hardware in the same data centre,

the company believes. “It provides significant performance improvements and cost savings over existing commercial hybrid quantum services,” it claims.

Bevan says this is a good example of early use cases. The quantum machine is based on photonics, and therefore can operate at room temperature. Couple this with the fact it is a new build data centre operated in partnership with a quantum start-up and the announcement still makes sense within the wider conservative approach to data centre investment.

Co-location and hybrid quantum data centres

But the rewards for bringing quantum data centres to life could be significant. Bringing quantum computers where the data is solves a number of security and latency concerns, says Stuart Woods, chief operating and strategy office for quantum-focused VC company Quantum Exponential. He is more bullish about the future of quantum computers in data centres and suggests the cloud makes it easier for companies to take risks.

“Six months ago you and I could go to AWS, Azure, IBM and get four different flavours of quantum computers,” he told *Tech Monitor*. “That is progress, but as I go from December to January this year the data centres are waking up. Equinix is an example where they installed loads of cloud computing and storage during Covid-19 and they ended up with more capacity than they needed.”

He said these data centres are slowly starting to realise that installing quantum hardware gives them another option. Quantum Exponential is an investor in Oxford Quantum Circuits, the partner Equinix worked with on its first quantum co-location in March. Woods says the benefit of having quantum hardware on site with real data is significant.

“Previously with AWS and others, we had to create exotic datasets, using synthetic data, to test on quantum computers as we couldn’t move the data across borders and most of the machines from companies like IBM, or on AWS where in a handful of countries. But now we’re in a new place where we are starting to see quantum computers arrive in data centres in locations where we have real-world data just one rack over.”

He said this means that an IT engineer working for a bank that hosts data in the Equinix Tokyo data centre will be able to run that data through quantum hardware. “That is what happened over the past four months and that is where I think things will evolve,” Woods says.

8.SES and TESAT to Develop Payload for Europe’s First Quantum Cryptography LEO Satellite System EAGLE-1

by Victoria-Louisa Kirstein and Suzanne Ong
https://www.ses.com/press-release/ses-and-tesat-develop-payload-europes-first-quantum-cryptography-leo-satellite-system

MEAGLE-1 consortium lead SES announces a new key partner, TESAT, responsible for developing and integrating the Quantum Key Distribution (QKD) payload for the EAGLE-1 satellite. The SES and TESAT partnership is aimed at achieving the next key milestone in building and implementing Europe’s pioneer-

ing quantum secure communications initiative EAGLE-1. Supported by the European Space Agency (ESA) and the European Commission, EAGLE-1 is a quantum key system integrating both space and ground segments that will deliver secure transmission of encryption keys across geographically dispersed areas and connect EU's national quantum communications infrastructures for truly sovereign networks.

Consortium member and Europe's leading laser communication technology company TESAT will manufacture the QKD payload comprising the Scalable Optical Terminal SCOT80 to establish a secure optical link from space to ground, as well as the QKD module of the satellite.

The technology integrated into the EAGLE-1 system's payload will include built-in redundancy and is specifically designed to be associated with the satellite communications and data transmission for such areas as government, telco operators, cloud providers and banking, to add guaranteed security of the cryptographic applications.

"EAGLE-1 is a project that will benefit the whole of Europe, and being able to work with the leading technology players in the market to co-develop it and together shape this innovative secure technology is a privilege to SES," said Ruy Pinto, Chief technology Officer of SES. "The addition of the secure optical links and the actual QKD module brings us closer to implementation, testing and further scaling the technology, that can ultimately serve millions of users. This elevates secure communications to an entirely new level, supporting development of reliable pan-European quantum communications infrastructures."

"We are delighted to be selected as payload prime by SES and looking forward to bring our expertise in integrating secure technologies, and a track record of almost 80,000 executed optical satellite links for the benefit of this highly-important and timely European project," said Thomas Reinartz, CEO of TESAT. "The EAGLE-1 system allows for achieving synergies together with leading industry partners, SMEs and institutes, reducing time to service and to market for the quantum secure technologies and its future key users, such as governments and institutions, or banking sector. Together with our partners, we are looking forward to strengthen European collaboration at all levels, including SMEs and institutions and contributing to European sovereignty in space."

About EAGLE-1

The EAGLE-1 project comprising satellite and ground infrastructure is developed by SES and its consortium of 20 European partners, and is co-funded by the ESA contribution of Germany, Luxembourg, Austria, Italy, the Netherlands, Switzerland, Belgium, and the Czech Republic under ARTES, as well as the European Commission through Horizon Europe.

Once launched in 2024, the EAGLE-1 satellite will complete three years of in-orbit mission. During the operational phase, the satellite will allow European Union governments and institutions as well as critical business sectors early access to long-distance QKD that would path the way towards an EU constellation enabling ultra-secure data transmissions.

9.Quantum Entanglement Shatters Einstein's Local Causality: The Future of Computing and Cryptography

by ETH ZURICH
https://scitechdaily.com/quantum-entanglement-shatters-einsteins-local-causality-the-future-of-computing-and-cryptography/

ETH Zurich researchers have succeeded in demonstrating that quantum mechanical objects that are far apart can be much more strongly correlated with each other than is possible in conventional systems. For this experiment, they used superconducting circuits for the first time.

- ETH Zurich researchers have made the first-ever loophole-free Bell test with superconducting circuits.
- They have confirmed that the conventional concepts of causality do not apply in the quantum world.
- For these experiments, they used a 30- meter-long tube whose interior is cooled to a temperature just above absolute zero (–273.15°C).

A group of researchers led by Andreas Wallraff, Professor of Solid State Physics at **ETH Zurich**, has performed a loophole-free Bell test to disprove the concept of "local causality" formulated by Albert Einstein in response to quantum mechanics. By showing that quantum mechanical objects that are far apart can be much more strongly correlated with each other than is possible in conventional systems, the researchers have provided further confirmation for quantum mechanics. What's special about this experiment is that the researchers were able for the first time to perform it using superconducting circuits, which are considered to be promising candidates for building powerful quantum computers.

An old dispute

A Bell test is based on an experimental setup that was initially devised as a thought experiment by British physicist John Bell in the 1960s. Bell wanted to settle a question that the greats of physics had already argued about in the 1930s: Are the predictions of quantum mechanics, which run completely counter to everyday intuition, correct, or do the conventional concepts of causality also apply in the atomic microcosm, as Albert Einstein believed?

To answer this question, Bell proposed to perform a random measurement on two entangled particles at the same time and check it against Bell's inequality. If Einstein's concept of local causality is true, these experiments will always satisfy Bell's inequality. By contrast, quantum mechanics predicts that they will violate it.

The last doubts dispelled

In the early 1970s, John Francis Clauser, who was awarded the Nobel Prize in Physics last year, and Stuart Freedman carried out the first practical Bell test. In their experiments, the two researchers were able to prove that Bell's inequality is indeed violated. But they had to make certain assumptions in their experiments to be able to conduct them in the first place. So, theoretically, it might still have been the case that Einstein was correct to be skeptical of quantum mechanics.

Over time, however, more and more of these loopholes could be closed. Finally, in 2015, various groups succeeded in conducting the first truly loophole-free Bell tests, thus finally settling the old dispute.

Promising applications

Wallraff's group can now confirm these results with a novel experiment. The work by the ETH re-

searchers published in the renowned scientific journal *Nature* shows that research on this topic is not concluded, despite the initial confirmation seven years ago. There are several reasons for this. For one thing, the ETH researchers' experiment confirms that superconducting circuits operate according to the laws of quantum mechanics too, even though they are much bigger than microscopic quantum objects such as photons or ions. The several hundred micrometer-sized electronic circuits made of superconducting materials and operated at microwave frequencies are referred to as macroscopic quantum objects.

For another thing, Bell tests also have a practical significance. "Modified Bell tests can be used in cryptography, for example, to demonstrate that information is actually transmitted in encrypted form," explains Simon Storz, a doctoral student in Wallraff's group. "With our approach, we can prove much more efficiently than is possible in other experimental setups that Bell's inequality is violated. That makes it particularly interesting for practical applications."

The search for a compromise

However, the researchers need a sophisticated test facility for this. Because for the Bell test to be truly loophole-free, they must ensure that no information can be exchanged between the two entangled circuits before the quantum measurements are complete. Since the fastest that information can be transmitted is at the speed of light, the measurement must take less time than it takes a light particle to travel from one circuit to another.

So, when setting up the experiment, it's important to strike a balance: the greater the distance between the two superconducting circuits, the more time is available for the measurement – and the more complex the experimental setup becomes. This is because the entire experiment must be conducted in a vacuum near absolute zero.

The ETH researchers have determined the shortest distance over which to perform a successful loophole-free Bell test to be around 33 meters, as it takes a light particle about 110 nanoseconds to travel this distance in a vacuum. That's a few nanoseconds more than it took the researchers to perform the experiment.

Thirty-meter vacuum

Wallraff's team has built an impressive facility in the underground passageways of the ETH campus. At each of its two ends is a cryostat containing a superconducting circuit. These two cooling apparatuses are connected by a 30- meter-long tube whose interior is cooled to a temperature just above absolute zero (–273.15°C).

Before the start of each measurement, a microwave photon is transmitted from one of the two superconducting circuits to the other so that the two circuits become entangled. Random number generators then decide which measurements are made on the two circuits as part of the Bell test. Next, the measurement results on both sides are compared.

Large- scale entanglement

After evaluating more than one million measurements, the researchers have shown with very high statistical certainty that Bell's inequality is violated in this experimental setup. In other words, they have confirmed that quantum mechanics also allows for non-local correlations in macroscopic electrical circuits and consequently that superconducting circuits can be entangled over a large distance. This opens up interesting possible applications in the field of distributed quantum computing and quantum cryptography.

Building the facility and carrying out the test was a challenge, Wallraff says. “We were able to finance the project over a period of six years with funding from an ERC Advanced Grant.” Just cooling the entire experimental setup to a temperature close to absolute zero takes considerable effort. “There are 1.3 tonnes of copper and 14,000 screws in our machine, as well as a great deal of physics knowledge and engineering know-how,” Wallraff says. He believes that it would in principle be possible to build facilities that overcome even greater distances in the same way. This technology could, for instance, be used to connect superconducting quantum computers over great distances.

10.IBM unveils end-to-end, quantum-safe tools to secure business, government data

by Michael Hill
https://www.csoonline.com/article/3695538/ibm-unveils-end-to-end-quantum-safe-tools-to-secure-business-government-data.html

Technology giant IBM has debuted a new set of tools and capabilities designed as an end-to-end, quantum-safe solution to secure organizations and governmental agencies as they head toward the post-quantum computing era. Announced at its annual Think conference in Orlando, Florida, Quantum Safe technology combines expertise across cryptography and critical infrastructure to address the potential future security risks that quantum computing poses, according to the company. IBM also unveiled the Quantum Safe Roadmap to guide industries along their journey to post-quantum cryptography.

Security experts and scientists predict that quantum computers will one day be able to break commonly used encryption methods rendering email, secure banking, cryptocurrencies, and communications systems vulnerable to significant cybersecurity threats. Organizations, technology providers, and internet standards will therefore soon be required to transition to quantum-safe encryption.

NATO has already begun testing quantum-safe solutions to investigate the feasibility and practicality of such technology for real-world implementations while the US National Institute of Standards and Technology (NIST) launched a competition to identify and standardize quantum-safe encryption algorithms. Furthermore, the US National Security Agency (NSA) announced new requirements for national security systems to transition to quantum-safe algorithms by 2025, and the White House released requirements for federal agencies to submit a cryptographic inventory of systems that could be vulnerable to cryptographically relevant quantum computers.

New capabilities prepare for post-quantum era in three ways

IBM’s new set of capabilities is designed to help clients prepare for the post-quantum era in three key ways, the firm said in a press release:

- IBM Quantum Safe Explorer enables organizations to scan source and object code to locate cryptographic assets, dependencies, vulnerabilities, and build a cryptography bill of materials (CBOM) that allows teams to view and aggregate potential risks into one central location.
- IBM Quantum Safe Advisor allows the creation of a dynamic or operational view of cryptographic inventory to guide remediation, analyzing cryptographic posture and compliance to prioritize risks.
- IBM Quantum Safe Remediator enables organizations to deploy and test best practice-based quantum-safe remediation patterns to understand the potential impacts on systems and assets as

they prepare to deploy quantum-safe solutions.

IBM Quantum Safe Roadmap charts milestones toward quantum-secure technology

The IBM Quantum Safe Roadmap is IBM's first blueprint that charts the technology milestones toward advanced quantum-safe technology, engineered to help organizations address anticipated cryptographic standards and requirements, and protect systems against emerging vulnerabilities, the firm stated. IBM said this is comprised of **three key actions**:

- Identify cryptography usage, analyzing dependencies, and generating a CBOM.
- Analyze the cryptography posture of vulnerabilities and prioritize remediation based on risks.
- Remediate and mitigate with crypto-agility (the ability to switch quickly between encryption mechanisms such as algorithms and cryptographic primitives while minimizing the impact on other systems) and built-in automation.

Quantum-safe encryption key to addressing quantum threats

Quantum-safe encryption is key to addressing the quantum-based cybersecurity threats of the future. Organizations are well advised to get ahead of the quantum-safe encryption curve, starting with understanding what data has the longest life and how this might be at risk from future threats. Companies that struggle should focus on identity, because even if they secure all their encryption, if someone can access their identity system, then anyone can gain "legitimate" access to systems and infrastructure.

Setting up years-to-quantum (Y2Q) migration as a bespoke project and giving it the firepower it needs to ensure success and a smooth transition is another key step, as is adopting a crypto-agile approach when thinking about any infrastructure overhaul. This means that organizations should use solutions that keep the tried and tested classical cryptography used today alongside one or more post-quantum algorithms, offering greater assurance against both traditional attacks and future threats.

11.Is your business quantum-safe? 6 questions you should be asking

by Alessandro Curioni
https://www.weforum.org/agenda/2023/05/6-key-questions-to-help-make-your-business-quantum-safe/

When it comes to encrypting sensitive data, the terms "post-quantum" and "quantum-safe" have become buzzwords. Particularly after the National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, announced four new algorithms poised to become new encryption standards in 2024.

As quantum computers continue to develop, processor qubits are increasing in number and becoming more stable – getting ready to take on complex problems deemed insurmountable for classical machines. But as quantum computers progress to their full potential, they also risk cracking modern encryption that could compromise sensitive data.

That's where quantum-safe cryptography – based on the mathematics of lattices – comes in. Unlike today's typical factor-based encryption techniques such as RSA, which relies on factoring complex, huge numbers, quantum-safe cryptography works instead with vectors – directions in a structured lattice.

The quantum threat to encryption is so serious that in May 2022, the White House issued a memorandum with the administration's plan to secure critical systems against future quantum computers. This was followed by the National Security Agency's (NSA) release of a new Commercial National Security Algorithm Suite (CNSA), detailing the use of new quantum-safe algorithms together with a timeline for replacement.

The World Economic Forum also estimated that in the next decade or two, more than 20 billion digital devices will have to be upgraded or replaced with these new forms of quantum-safe encrypted communication.

Some industries have already begun planning for the switch to quantum-safe protocols. Telecommunications industry organization GSMA formed a Post-Quantum Telco Network Taskforce last September, with IBM and Vodafone joining as initial members. The aim is to help define policy, regulations and operator business processes to protect telcos from future quantum threats.

The taskforce recently published a *Post Quantum Telco Network Impact Assessment*, an in-depth analysis of the quantum security threats facing the telecommunications industry and a detailed list of potential solutions to prepare for these threats.

While there's been a lot of chatter about businesses being urged to "go quantum-safe", for a typical company those words may raise more questions than answers. At IBM, we're addressing them with a "quantum-safe roadmap" that takes organizations through the phases of discovery, observation, and transformation.

Here are the answers to six key questions to help you make your business quantum-safe.

1. How would you "discover" which data and systems to migrate to new algorithms?

Each company will have its own priorities when it comes to what to migrate and when. For some, it will be necessary to migrate to continue selling products and services to the US federal government. For others, it may be the risk that a future quantum event may put them out of business, for example in the case of a data breach. So first, it's important to understand where and how old algorithms are used and to analyze the risks involved. This is ideally achieved through extending the use of secure software supply chain concepts that have also been the subject of an Executive Order on Improving the Nation's Cybersecurity.

To help organizations at this initial stage, IBM developed a tool called Explorer, which scans the source code and object code to surface all cryptographically relevant artefacts, pinpoint their locations, and uncover dependencies. Explorer generates a call graph that catalogues cryptographic artefacts, producing a knowledge base that is arranged into a Cryptography Bill of Materials (CBOM).

2. How do you "observe" your organization's data and systems priorities?

In the "observe" stage, an organization takes what has been discovered and generates a cryptographic inventory enriched with context, to analyze the cryptographic state of compliance. This inventory provides a list of vulnerabilities based on industry-specific compliance policies and

business priorities so an organization can more easily update its cryptographic infrastructure.

For this stage, we developed a tool called Advisor. It integrates with network and security scanners in an organization's IT environment to consolidate and manage CBOMs and collect metadata from other network components to generate a comprehensive cryptographic inventory. With policy-based data, Advisor can generate a list of at-risk assets and data flows that equip businesses to analyze their cryptographic compliance status.

Companies can save cost and effort by aligning strategic modernization initiatives that simplify crypto migration and enhance security. A strategy that combines risk with strategic application modernization is the best route to becoming quantum-safe.

3. How long will the quantum-safe "transformation" take?

It depends on what is being migrated. A complex legacy system may be very difficult to migrate. Application modernization is key in the journey to quantum safety.

When an organization is ready to "transform," we have Remediator: a tool that allows businesses to test quantum-safe remediation patterns so that they understand the potential impact on systems and assets. Remediator helps address any pattern that suits the organization to be quantum safe.

It allows the organization to work with different quantum-safe algorithms, certificates and key management services. And it helps them to quickly adapt to changing policies and threats without significant operational or budgetary implications. Remediator also supports a hybrid implementation approach that allows organizations to use classical and quantum-safe cryptography in their transition toward quantum-safe algorithms.

4. Can the transformation be done in the background of your normal operations?

With the right awareness and strategic governance, it is possible to gradually migrate a company with minimum impact. Take for example APIs that an enterprise might use internally or offer externally. It is very straightforward to use quantum-safe-enabled infrastructure components that provide access to these APIs, protected with quantum-safe algorithms. IBM used this approach to offer a second quantum-safe gateway to its IBM Cloud Key Protect services.

5. What are the new NIST algorithms, and how do we know they really are more secure?

The best way to think about these algorithms is as the next generation of cryptographic algorithms. They have now been selected for future US federal use and will find their way into many other countries' and industries' regulations. The algorithms were developed by external consortia from around the world and submitted to a competition organized by NIST. This six-year process led to intense and open scrutiny of the algorithms and to four candidates being selected by NIST for standardization by 2024.

6. Why should you invest in this migration now, when quantum computers are not yet fully practical?

We don't know when a cryptographically-relevant quantum computer will be developed. But a new generation of cryptography to protect against this future is already here. The adoption of

quantum-safe cryptography is finding its way into legislation and ecosystems, and most companies will have to support it.

Starting this journey today through awareness of the need to migrate at a strategic level has many advantages. Steps that simplify migration can be added to existing security initiatives and application modernization programs. This will minimize effort and save costs in the long run. Waiting, on the other hand, means that more at-risk legacy is being created, making it more difficult to eventually migrate.

That's why you should start the journey to quantum-safe algorithms today.

12.10 companies building quantum computers

by Jacob Roundy
https://www.techtarget.com/searchdatacenter/feature/Companies-building-quantum-computers

Many organizations are paving the road to a future built on quantum computing, and that future is a promising one. With quantum computers at our fingertips, humanity will be able to solve hugely complex problems at scale and faster than ever.

However, getting to that future has a significant amount of roadblocks to overcome first before quantum computing becomes widely available. Many companies -- of all sizes -- are actively developing and building quantum computers and capabilities.

Companies building quantum computers

As quantum computing continues to develop and undergo research, companies are building quantum capabilities in both hardware and software. Companies in this list are developing quantum capabilities in various ways, including infrastructure, algorithms and development environments for testing.

While this list is not exhaustive, here are some of the companies building quantum computers.

- **Amazon**

  Amazon is a more recent player joining the race to build a quantum computer. In 2021, Amazon announced the opening of the AWS Center for Quantum Computing in Pasadena, Calif. It has partnered with the California Institute of Technology to foster the next generation of quantum scientists and fuel their efforts to build a fault-tolerant quantum computer.

  In addition to these efforts, Amazon offers a quantum computing service called Amazon Braket, which provides developers access to quantum computers and tools from third-party partners. This service enables customers to speed up their own quantum computing research, build quantum projects and run quantum algorithms.

- **D-Wave Systems**

  D-Wave Systems, a Canada-based company, is the world's first organization to sell a commercial quantum computer. Its latest, the D-Wave Advantage system, features a processor architecture

with more than 5,000 qubits and 15-way qubit connectivity.

D-Wave's quantum computers use a process called *quantum annealing*. This process is specifically designed for optimization, so when users map a problem into a search, the processing unit considers all possibilities simultaneously and presents calculations that correspond to the optimal configurations of qubits found. These values are the best possible outcomes, resulting in higher-quality results at scale.

D-Wave is currently developing an incremental follow-up to the Advantage system. In addition to hardware, the company offers a cloud-based full stack of systems to enable enterprises, government agencies, national laboratories and academic organizations to build quantum applications.

- **Google**

Google's Quantum AI lab has been developing a programmable superconducting processor. A recent iteration is Sycamore, a 54-qubit processor composed of high-fidelity quantum logic gates.

In 2019, Google claimed Sycamore had achieved quantum supremacy. Quantum supremacy is the point at which a quantum device can solve a problem exponentially faster than a classical processor. In this case, Sycamore took about 200 seconds to sample one instance of a quantum circuit 1 million times -- something that would have taken a classical supercomputer nearly 10,000 years to do.

Since then, Sycamore has been used to run chemical simulations, wormhole simulations and more. Google has also developed a software stack of open source tools and a quantum computing service to develop novel quantum algorithms. Its research team is continuing to push innovation in quantum computing, from hardware control systems and quantum control to physics modeling and quantum error correction.

- **IBM**

In November 2022, IBM held the Quantum Summit, where it unveiled a development roadmap detailing its plans and timeline for progressing quantum computing through 2025. Its primary goal is to go beyond using single processors, and by 2025, it plans to combine multichip processors into what it has named the Kookaburra processor. Compared to IBM's latest processor, Osprey, which has 433 qubits, IBM plans for the multichip Kookaburra processor to have 4,158 qubits.

These plans are ambitious, but IBM has a strong history in quantum development. In 2019, it launched a commercial quantum computer, the IBM Quantum System One. It's currently developing the IBM Quantum System Two to better serve Osprey and future quantum processors.

In addition to hardware, IBM runs a suite of cloud-based quantum systems, providing researchers, organizations and developers with access to various services and resources, including IBM Quantum Composer, IBM Quantum Lab and Qiskit, an open source SDK for quantum computers. This platform has both public and premium tiers for users to develop, test and run quantum projects.

- **IonQ**

IonQ's quantum computers use trapped-ion technology. Most quantum hardware uses synthetic quantum systems for its qubits, but IonQ uses naturally occurring individual atomic ions at the core of its processing units. These ions are trapped in a 3D space, and IonQ uses lasers to help prepare and perform the calculations.

IonQ has three quantum systems: IonQ Harmony, an 11-qubit system that launched in 2020; IonQ Aria, a 25-qubit system that launched in 2022; and IonQ Forte, a 32-qubit system that's currently under development and in beta testing with researchers. All are based on IonQ's trapped-ion technology architecture, and Harmony and Aria are available through IonQ Quantum Cloud or Amazon Braket.

Microsoft

Microsoft is currently developing its own scalable, full-stack quantum machine with a unique approach that's focused on topological qubits. The research team at Microsoft has invented a control chip, called Gooseberry, and a cryo-compute core that are key to this approach.

In short, the chip and core work together to maintain a stable cold environment that enables the quantum stack to send and receive information to and from every qubit. Achieving this task is no simple feat; however, if Microsoft can pull it off, it will result in a highly scalable quantum computer that can support even larger, more complex applications.

While development is still ongoing for this hardware, Microsoft also offers a portfolio of quantum computers from other hardware providers as part of its Azure Quantum platform. This service provides an open development environment for researchers, businesses and developers that enables the flexibility to tune algorithms and explore today's quantum systems.

QCI

Quantum Computing Inc. (QCI) is a full-stack quantum company that claims to be committed to democratizing access to quantum value. Rather than building quantum computing services for the largest of enterprises, QCI's offerings are more affordable and can be used by non-quantum experts.

From a hardware perspective, QCI has built the Entropy Quantum Computer (EQC), which aims to create useful qubits to perform computations today rather than 10 years in the future. Organizations can use an EQC through a two-tier subscription service: Dirac-1, a qubit-based system, and Dirac-2, a qudit-based system.

QCI also offers Qatalyst, a cloud-based service that enables end users to solve problems on quantum systems without requiring complex programming knowledge. In line with this is its QUBT University, which helps users learn about quantum algorithms and how to run computations. QCI is currently developing new quantum computing chip capabilities.

Quantinuum

In 2021, Honeywell Quantum Solutions and Cambridge Quantum announced a merger, forming Quantinuum. The merger brought together Cambridge Quantum, a developer of quantum software, and Honeywell Quantum Solutions, which builds quantum hardware based on trapped-ion technologies.

Honeywell's quantum computer, the System Model H1, has achieved the highest quantum volume measurement -- 32,768 -- in the history of quantum computing. This hardware pairs with Cambridge Quantum's software package, which applies quantum computing to solve complex problems across industries, from pharmaceuticals to specialty chemicals and beyond.

- **Rigetti Computing**

  Rigetti Computing is an integrated systems company that builds quantum computers and superconducting quantum processors. Its most recent processor, the Aspen-M-3, has 80 qubits and is based on multichip technology. Its quantum processors are universal, gate-model machines.

  Rigetti is currently developing a new 84-qubit processor called Ankaa, and the plan is to put four of these processors together to form a 336-qubit machine named Lyra. Its roadmap includes building an even larger machine that can support 1,000 qubits in 2025 and one with 4,000 qubits in 2027.

  Users can access Rigetti's quantum computing systems through its Quantum Cloud Services platform or Amazon Braket. The cloud platform enables coders to write quantum algorithms for simulations of their quantum chips.

- **Xanadu**

  Xanadu Quantum Technologies is a Canada-based company that's taking a photonic approach to building quantum computers.

  Xanadu's Borealis, one of the largest photonic quantum computers every built, uses photonics and quantum light sources that emit squeezed-light pulses. The Borealis features more than 216 squeezed-state qubits and is particularly effective at solving Gaussian boson sampling problems -- something that would take classical computers thousands of years to do.

  Xanadu also leads the development of PennyLane, an open source software library for quantum computing and application development. Organizations can access Borealis through Xanadu Cloud or Amazon Braket.

13.Encryption: The Necessary Tool For U.S. National Security And The Intelligence Community

by Gary Weinstein
https://www.forbes.com/sites/digital-assets/2023/05/07/encryption-the-necessary-tool-for-us-national-security-and-the-intelligence-community/amp/

Importance of Encryption in National Security

A key need for the intelligence community to prioritize the advancement and adoption of encryption technologies to bolster national security arises from the escalating use of digital repression strategies by authoritarian regimes. China, for example, leads the world in applying surveillance and censorship to monitor its population, repress dissent, and strengthen its surveillance and security apparatus. The rise of digital authoritarianism and the increasing sophistication of surveillance technologies pose substantial threats to democratic values and individual privacy.

In addition to combating digital repression, addressing rapid technological advancements is another vital

aspect of national security interests. Adversarial foreign intelligence services are embracing cutting-edge technologies such as generative artificial intelligence, cyber tools, unmanned systems, and advanced technical surveillance equipment, thereby enhancing their capabilities and challenging U.S. defenses. Alarmingly, the thriving commercial spyware industry, currently valued at approximately $12 billion, is experiencing rapid expansion, with authoritarian governments increasingly weaponizing spyware.

Given these challenges, the U.S. intelligence community should emphasize the development and implementation of encryption technologies, such as end-to-end encryption, to protect individual privacy and preserve democratic values. End-to-end encryption has already been recognized as a vital tool for safeguarding human rights by the United Nations, and numerous UN resolutions have highlighted encryption's importance in this regard.

As an illustration of encryption's importance, the U.S. government recommended its adoption for secure remote work during the Covid-19 pandemic. The National Security Agency issued guidance, vigorously endorsing the use of end-to-end encryption for government employees and military personnel, highlighting the role of encryption in ensuring secure communications.

By concentrating on encryption technologies, intelligence communities can counter the spread of repressive technologies and protect individuals from the invasive surveillance tactics employed by authoritarian governments. This is particularly important in the context of financial privacy, as the development and use of privacy-preserving technologies can help individuals safeguard their financial transactions and limit third-party access to their data.

Intelligence Community's Encryption Use Cases

There are many use cases for encryption technologies within the intelligence community. One powerful use case is facilitating secure payments to assets or "spies." By utilizing encrypted digital cash, the identity of both the intelligence agency and the asset can be effectively protected, ensuring the confidentiality of sensitive operations. This secure method of payment is critical in maintaining the anonymity of those involved, thus reducing the risk of exposure and potential harm to the asset or the agency's operations.

And, encryption technologies provide a powerful tool in creating secure communication channels. By implementing strong encryption, sensitive information exchange between agents, analysts, and decision-makers can be protected from interception by adversaries. This ensures that vital intelligence and operational details remain confidential, preserving the security of ongoing missions and strategic planning.

In addition to securing communication channels, encryption technologies are essential for protecting the vast amounts of sensitive data collected and stored by intelligence agencies. Classified information on national security threats, details of covert operations, and other critical data can be safeguarded using advanced encryption techniques. This protection is vital in preventing unauthorized access or cyberattacks that could compromise national security interests.

Encryption technologies also play a crucial role in anonymizing the online activities of agents and analysts when conducting investigations or infiltrating digital platforms used by adversaries. Tools such as virtual private networks, Tor networks, or other anonymizing technologies can be utilized to encrypt and obfuscate users' digital footprints, making it difficult for adversaries to track or identify them.

Safeguarding supply chain security is another essential use case for encryption technologies. By employing encryption to secure communication and data transfer between suppliers, manufacturers, and intelligence agencies, the integrity and confidentiality of sensitive components, materials, and equipment utilized by the intelligence community can be protected from tampering or interception.

Enhancing biometric security is yet another application of encryption technologies in the intelligence community. Agencies often use biometric data, such as fingerprints, facial recognition, or voice patterns, for identification and access control purposes. By employing encryption techniques, they can protect this sensitive biometric data, preventing unauthorized access, identity theft, or other security breaches that could compromise personnel or operations.

Prioritizing Encryption Research And Development

As part of these efforts, the intelligence community should prioritize research and development in encryption technologies to stay ahead of adversaries in the constantly evolving cyber landscape. This includes investing in cutting-edge encryption methods, training personnel in encryption best practices, and sharing relevant expertise with democratic partners around the world. These efforts demand immediate attention.

In light of the unclassified Annual Threat Assessment of the U.S. Intelligence Community from February 6, 2023, encryption technologies are essential for safeguarding national security interests in a world dominated by strategic challenges, such as competition between great powers, rising regional powers, and evolving non-state actors. The threat assessment highlights the increasing influence of authoritarian governments that seek to reshape global norms and challenge democratic values. By prioritizing the development and implementation of encryption technologies, the U.S. intelligence community can better protect national security interests and maintain an advantage in the face of these strategic challenges, while also promoting democratic principles and individual privacy.

And, in a recent Senate Armed Services Committee hearing on May 4, 2023, Lt. Gen. Scott Berrier, Director of the Defense Intelligence Agency, in his annual threat testimony, emphasized the importance of adapting to the complex threat landscape posed by strategic competition with countries like China. Director Berrier warned, “China is our pacing challenge and DIA’s Top Priority” and highlighted the ongoing transformation of DIA to better address these challenges. This testimony underscores the urgent need for the intelligence community to prioritize the development and implementation of encryption technologies to safeguard national security interests and counter the growing threats of digital authoritarianism in the face of such strategic competition.

Rising Commercial Spyware Threats And Surveillance

A revealing instance of commercial spyware misuse was reported on July 19, 2021, when a consortium of international news outlets, including The Guardian and The Washington Post, disclosed findings from an investigation into NSO Group’s Pegasus spyware. As described in MIT Technology Review, tens of thousands of phone numbers were found to be targeted by Pegasus, with journalists and activists from numerous countries being surveilled, despite NSO Group’s claims that their spyware is designed to target criminals and terrorists. In a recent report published by Citizen Lab on April 18, 2023, the evolving attack techniques of NSO Group’s Pegasus spyware were highlighted as a significant concern for digital privacy and security. Pegasus has become increasingly sophisticated, using zero-click exploits and multiple attack surfaces to compromise devices, making it a considerable threat to individuals and organizations. As the Citizen Lab report states, “NSO Group’s Pegasus spyware remains a threat, and their attack techniques continue to evolve.”

And, in a lawsuit filed on November 30, 2022, in the US District Court, Northern District of California, the dangerous capabilities of Pegasus spyware were extensively detailed by plaintiffs consisting of the journalists and staff of El Faro, a prominent Central American digital newspaper known for their fearless investigative journalism. According to the complaint, Pegasus is notorious for enabling operators to remotely and covertly control a target’s smartphone and extract data without the user’s knowledge or consent. The lawsuit highlights the immense threat that Pegasus poses to press freedom and human rights,

as it has been sold to authoritarian governments and used to target journalists, activists, and political opponents globally. This case underscores the urgent need for increased vigilance and protective measures to defend against the growing threat of advanced surveillance technology and the emergence of new forms of commercial spyware.

Strengthening National Security With Encryption

Ultimately, encryption technologies offer a strong and effective shield against the escalating risks of digital repression, safeguarding democratic principles and personal privacy. As digital authoritarianism intensifies and surveillance technologies become more advanced, embracing, cultivating, and deploying encryption technologies will bolster national security efforts. This will contribute to a safer, more democratic future for all.

14.Quantum computing race explained: fast and furious

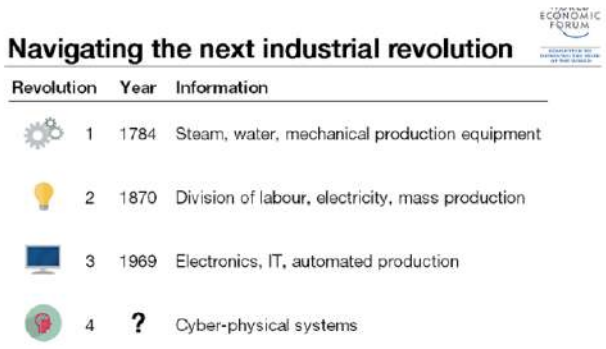
by Stefanie Schappert
https://cybernews.com/editorial/quantum-computing-race-explained/

The World Economic Forum (WEF) published several think pieces this year describing a post-quantum computing world in which the global chasm between developed and underdeveloped populations only grows larger. But could the gloomy forecast be rosier than expected?

Between Twitter's Elon Musk and Apple's Steve Wozniak calling for a six-month pause on AI development, threats of mass job extinction, claims of sentience, and now the proclaimed "godfather of AI" Geoffrey Hinton quitting Google so he can warn of its dangers, public confidence in advanced technology is muted at best.

However, Cybernews found one industry insider with a glass-half full approach, making the unavoidable leap into the quantum field seem much more palatable.

Four is the magic number



The threat of digital inequalities plaguing entire nations echoes sentiments from scholars, economists, and geopolitical analysts alike, as expressed by WEF Founder and Executive Chairman Klaus Schwab.

He and his colleagues believe the inevitable coming of what is being called the Fourth Industrial Revolution will not only fundamentally transform “the way we live, work, and relate to one another,” but create a “quantum divide” among humankind that could negatively impact history in ways never imagined.
My colleague Damien Black published his own insider interview piece earlier this year, finding similar viewpoints between Protiviti’s quantum computing director Konstantinos Karagiannis and the WEF.

So when I spoke with Matt Johnson, co-founder and CEO of quantum computing development firm QC Ware, it was refreshing to hear an alternate take.

Johnson – a former intel systems Air Force captain and finance executive who took the plunge into quantum nearly a decade ago – described a world stage where, despite its challenges, quantum computing will be more accessible than ever, even to those nations struggling economically to invest in advanced technology.

Touching upon the quantum divide, policy vs funding, the race with China, encryption algorithms, and the almighty cloud, Johnson believes the key to ensuring future quantum technologies reach all levels of society will rely heavily on collaboration between the public and private sectors within nations already leading the way.

Do you believe quantum computing is bringing the world closer together or pushing it further apart?

The first thing that comes to mind is that quantum computing, which is a form of high performance computing, is being aggregated into the divide where the United States is putting up hard kind of borders around export of these critical technologies and semiconductors and quantum computing.

And so, yes, in areas where it's geopolitically tough, it's putting up boundaries. On the other hand, the United States is just as aggressively reaching out to partner with what they would call like-minded countries.

I think the US, if you want to consider this from a policy level, is being extremely pragmatic about this technology and saying, if we look back at the 20th century around information technology and nuclear technology, it's never been one country that's been able to pull it off. It's generally a consortium of experts from around the world.

So you do see at the governmental level, and kind of quasi governmental level, a lot of bridges being built for the quantum computer.

Would you say that those bridges are being built necessarily within our borders and with private companies? Or are you talking about other countries specifically, such as in Europe?

Other countries, certainly government-to-government agreements that are being signed. It's all about trying to jointly accelerate technology development for quantum.

Now on the private sector side, there's never borders that exist there. I mean, unless the US government said, you can't go there. Money flows to wherever there's going to be a positive return. In our case, for instance, I guess probably 70% of our customer base is non-US.

A lot of European and Asian corporations, they look backwards on other emerging technologies, such as machine learning, and they perceive there to have been historically a technology gradient between where the US is and where Asia or Europe are. And it’s something that has caused them to double down on investments into US startups or tech. If you look at the composition of investors, I think quantum enjoys a lot of non-US money.

The WEF focuses on the divide between China, the US and other countries, specifically regarding quantum investments. China has the most at $15 billion, while the US and Europe combined constituted a close second at around $10 billion. But besides the 17 nations that have "national initiative or strategy to support quantum technology research and development," more than 150 countries do not. So, it's interesting that you're saying a lot of non-US countries are investing in quantum technology. Do you think that means there will be some information sharing, but that it is ultimately our responsibility to share the technology once it's more advanced?

Sure. Just like every technology. You could, if you have a corporate conscience, of course. I think you'll find responsible corporations will definitely be doing that. And by the way, there's money there as well. So there's a financial incentive.

I don't see quantum computing explicitly as being a technology that is going to be less or more adopted by the developing world than any other new technology. There's a reason to bring information technology across all borders to prop up the entire global community.

There's been a lot of fear-based talk about something like another Cold War nuclear arms race between China and America.

You're right about that. And there's nothing that private sector companies can do. On the other hand, [while] the walls are being put up around China or North Korea, just the opposite is happening with the rest of the world. Like the EU and the US, as more democratic free-market areas, are always pushing hard to build bridges. Markets that you can sell into or that you can draw brainpower out of, tap into sources.

Is this because China has government control over its private industry? It seems it can cherry-pick a lot of technology from companies and put it all together in a way that the Western world does not, especially the United States, being that our private companies tend to keep a lot of theirs secret. Do you foresee the US government forcing them to share, to keep up in the technology race between East and West?

Well, certainly I would love to see them stimulate more. Right now, the US government, through National Quantum Initiative, has been very active and visible at the policy level. But at the funding level, what the government is putting into quantum technologies pales in comparison to what China is doing. I think there's a direct correlation between the amount of capital invested in the new technology and the rate that it gets developed and fielded.

On the one hand, the US has said quantum technologies are critical to national competitiveness and security. And on the other hand, there's just not a lot of money flowing from them [US government] to support that.

It almost seems like they're expecting the private companies to pick up the slack, so to speak, in that regard?

And that doesn't work well with fundamental research. It works well with applied research and product development: that's where the private sector is able to take risk. [But] historically, the moonshot, the nuclear weapons program, this is all government funding. I think it's a real problem.

Possibly in the next ten years, quantum will be able to break a lot of current encryption systems. Nefarious actors are now harvesting data, saving it until that time. That is going to affect not just government security but private companies in regard to intellectual property (IP) and whatnot. Do you think the government is hoping that companies are going to find ways to prevent that for their own interests?

Actually, I don't. I think the government, like agencies that care about cryptography, are alerted to this. They're trying to collaborate with industry to educate them on how to protect themselves against this impending threat.

But again, what I sense is that there's not much visible activity by the US government at all in this. Even though it's been described as a high priority, I don't see any action.

What do you think the ramifications of that will be in the future if we're not keeping up with China on this?

That's a leading question. Our sensitive data, intellectual property, those things could be at risk.

And there are other countries around the world who have traditionally adopted a very lazy way of innovating, and that is by stealing our innovation. And it's very, very harmful to the US.

So, that's the consequence, right? It would be a very serious economic shock.

Some experts even say breaking encryption with quantum computers could happen in as little as three years. Do you think that is a realistic expectation?

There's one quantum algorithm out there that has been proven to be able to crack encryption. It's called Shor's algorithm. If you look at the size of the quantum computer you'd need to run that and break a real live key, it seems unlikely you'd have one large enough in the next three years. Anything outside of three years I think is possible, but speculative. You really don't know.

Now, the real threat is that there would be other quantum algorithms developed alongside Shor's which could do this kind of work with smaller computers that will be coming online. Developing algorithms is not that expensive. I'm sure every country around the world is trying to do that. I mean, there's a huge incentive for it. From their perspective, It's like treasure hunting.

This would mean there is a huge incentive for cybercriminals to do the same thing?

Yes.

What of the socio-economic differences between countries that have programs to develop this technology? There are still countries that have issues even with being online: the WEF says 2.9 billion people are still offline and do not benefit from the digital economy. What do you think about the implications of this in health, medical advancements, education, energy, infrastructure, transportation, and so on? Will less-developed countries not be able to access quantum resources?

The way quantum computing systems are architected, they will attach to the cloud. So you won't need to wheel a quantum computer physically to a country that's impoverished.

What you will need is basic access to the internet. And that would allow this powerful resource to be disseminated to those countries. And of course, you'll be able to purchase quantum computing power on kind of a pay-as-you-drink basis through Amazon or Google Cloud.

You can tap into that power for very little money, thanks to cloud computing. Thanks to a distributed internet that problem you're describing can be mitigated. The real key, frankly, is just to have more internet connectivity in those countries.

I firmly believe the issue is not that quantum computing will be too expensive or inaccessible. These machines will become easier to use over the next couple of years. There will be methods of utilizing quantum power for very little money. So there's nothing peculiar to quantum computing that would make it onerous to get into those [underprivileged] parts of the world.

But when it comes to developing the actual technology in the first place, do you think that is where the race is going on between East and West?

Yes, I definitely do. It's heating up. It's this potent technology: frankly I don't think anyone under any government really understands precisely what quantum computing will be useful for.

Certainly the industry and community talk about artificial intelligence and how quantum computing could be used for that. Think about that again at a nation-state level: the AI thing, that specter that is at once an opportunity and a threat. That's what people in government associate quantum computing with.

But coming back to the race, when it really accelerates is when those use cases, machine learning, material design, drug discovery, are validated a little bit more. Then that race would really heat up.

So you're saying once that information is discovered, it's going to be out there – easily available to other nations who aren't necessarily making the discoveries themselves?

Possibly, yeah. Look at the semiconductor industry. For several decades, Western allies including Taiwan have had a near-monopoly on the most advanced integrated circuits and chips. They've done that by very aggressively protecting their IP [intellectual property]. I think the same thing applies to quantum computing: there will be very aggressive protection of IP.

15."The Time for Quantum is Now." Quantum Exponential's New COO Stuart Woods, is on a Mission to Nurture the Sector

by Stuart Woods
https://thequantuminsider.com/2023/05/05/the-time-for-quantum-is-now-quantum-exponentials-new-coo-stuart-woods-is-on-a-mission-to-nurture-the-sector/

Stuart Woods is the newly appointed Chief Operating Officer of Quantum Exponential. He has more than 30 years of experience leading technology companies, ranging from startups to publicly traded, multi-million-pound businesses. Previously Managing Director at Oxford Instruments NanoScience, Stuart explains why he is excited to move from an operational commercial role in the quantum industry to investing in quantum startups.

When you're sitting on a technology curve that is as steep as we are experiencing now, the only way that we can see change is by looking backwards. I fundamentally believe that's where we are with quantum. We're climbing up the face of a mountain.

Where we are on the curve

Having lived through the telecoms boom – and having left my advanced degree study in organic chemistry, in what is now called computational chemistry, to work in telecoms – I can see clear parallels with quantum technology today. We now take it for granted that we have high-speed internet, broadband and wifi, but at the height of the telecoms boom in the early 2020s, they just didn't exist. In the same way, with quantum, I don't see why in the next ten years we won't be living with quantum technologies that are unimaginable now.

In fact, there is a fundamental difference between what happened in the telecom boom and what will happen with quantum that makes it even more exciting. At no point before in human history have we been able to take cutting edge technology and immediately share it with millions of people – through cloud access. That element of broad democratisation and availability of the technology means we're able to question and correct our developments more quickly and thoroughly than ever before – while also exploring channels to market and product configurations for specific applications at lower cost points. It gives us much better safeguards against failure and I truly believe that for investors, the time is now for quantum – it is an asset class needed by all portfolios.

Although quantum computing gets most of the media attention, quantum technologies encompass sensing, networks, encryption and infrastructure. Each one is at a different stage of development. I believe we will see successes in quantum sensing a lot earlier than complete and total successes for computing. There is an element of maturity that we're yet to see with quantum computing. However, we may have the ability to use quantum sensors to understand geographical phenomena like subsidence and sinkholes as soon as within the next year. Just as autonomous vehicles drove professional mapping to the consumer – which led to easier travel – quantum sensors will lead to an understanding of the planet which will heighten and focus the immediacy of climate change.

Applying commercial experience to investment

Progress in any area of quantum can only be achieved with the correct investment. My career so far has been within the product and commercial side of technology businesses, so moving to the financial side is a chance to make changes with an outsider's perspective and understanding of what can be commercialised and what business models work for different technology products. I know that finance could be made more efficient and that different companies at different levels of maturity could benefit from a more positive and constructive finance environment with venture capital.

I think that is one of the strengths of the team at Quantum Exponential, there is a balance between commercial, technical, and operational understanding. When you bring those together, I believe you can then provide a truly full service of venture capital funding – and this is exactly what quantum needs. We can provide the right investments to startups in such a way that they're synergistic, and cooperate well within an ecosystem together; we can create a market at scale providing a return on investment.

What makes a successful quantum startup

A business needs a good product, a customer and a channel. For businesses in the quantum computing space, cloud access to quantum is crucial in developing the market. For almost all businesses, having a quantum computer will be out of reach, so accessing quantum compute power through the cloud from IBM, Microsoft, Amazon, Google, or your own cloud will be the standard route to market. Even sensor solutions can be cloud enabled – most large scale mines or even the London Tube network is remotely monitored as a service. Never forget that selling a product over a service comes with more costs and limits your short term roadmap options.

In any area of quantum technology, assuming that the business is working on a viable idea, the dynam-

ics of the team are the biggest indicator of whether a startup will succeed or fail. The importance of teamwork just can't be overstated. In a fast-paced business with high risks, the first job of the founder is to build a positive team. Then to nurture that team with a shared vision, good communication and high levels of trust. Your team will be stress-tested daily and you will have to deal with failure more often than success. If you need to second guess your team then you've lost.

Ultimately, it doesn't matter what your company is or what you're doing, it's the potential of your people and team that will result in your success. Through acquisitions and financial investment, you are investing in people. And that's why I'm very passionate about joining the team at Quantum Exponential.

16.D-Wave Quantum Annealer Practical Usage in 2023

by James Dargan
https://thequantuminsider.com/2023/05/05/d-wave-quantum-annealer-practical-usage-in-2023/

What is a Quantum Annealer?

By utilizing properties specific to quantum physics such as quantum tunnelling, entanglement, and superposition, quantum annealing (QA) (related to adiabatic quantum computation) is a method for solving problems involving a large number of possible solutions and variables.

The purpose of quantum annealing is to solve optimization problems using adiabatic quantum computing. The optimization problem is solved by gradually transforming a simple quantum state — called the initial state — into a more complicated quantum state that encodes the solution. Hamiltonians are mathematical operators that describe the energy of a quantum system and control the transformation. Throughout the process of transformation, the system tends to settle into a state with the lowest energy, which corresponds to the solution of the optimization problem.

In contrast, adiabatic quantum computing uses quantum computers to solve a wide range of problems. As a result, a simple quantum state is gradually transformed into a more complicated quantum state which encodes the solution. As in quantum annealing, the transformation is controlled by a Hamiltonian. It doesn't necessarily have to be designed specifically for optimization problems, since the transformation can be more general.

As one of the pioneers of quantum computing, D-Wave uses QA, an optimization process that uses quantum fluctuations for determining a given objective function's global minimum.

Last summer, D-Wave made the announcement of a prototype of the next-generation Advantage2 annealing quantum computer in the Leap quantum cloud service. Using an innovative new qubit design and the new Zephyr topology, the D-Wave prototype has over 500 qubits, which features 20-way connectivity.

In under a year, however, the company has improved upon last year's numbers, as D-Wave shared progress toward its next-generation Advantage2 annealing quantum computing system, which will feature 7000+ qubits and 20-way connectivity, and is expected to be implemented in a lower-noise fabrication stack, so customers could solve more complex problems more precisely.

Modern technology is allowing quantum annealing to become a commercial reality. Compared to tradi-

tional computers, it is claimed to be more effective at solving optimization problems with a large number of local minima.

In addition to taking place in the laboratory, it is a promising quantum technology for companies that have serious optimization problems that are too difficult for traditional computers to solve.

What Are Some Applications of Quantum Annealing?

As already mentioned, quantum annealing is best suited to optimization problems. A good use case showcasing this is described in the paper *Application of Quantum Annealing to Nurse Scheduling Problem*, published in Scientific Reports by Kazuki Ikeda, Yuma Nakamura and Travis S. Humble in 2019.

The three detail that there is considerable interest in quantifying quantum annealing's performance on real-world problems in order to gain insight into how this approach can be most effectively applied in practice. Using the D-Wave 2000Q quantum annealing device, the researchers investigated the empirical performance of quantum annealing in solving the Nurse Scheduling Problem (NSP) with hard constraints. Under a set of schedule and personnel constraints, NSP seeks to assign nurses to shifts optimally. They worked out that by reducing NSP to a novel Ising-type Hamiltonian, they could evaluate the solution quality obtained from the D-Wave 2000Q against the constraint requirements.

The abstract of the paper ends:

"*For the test problems explored here, our results indicate that quantum annealing recovers satisfying solutions for NSP and suggests the heuristic method is potentially achievable for practical use. Moreover, we observe that solution quality can be greatly improved through the use of reverse annealing, in which it is possible to refine returned results by using the annealing process a second time. We compare the performance of NSP using both forward and reverse annealing methods and describe how this approach might be used in practice.*"

Difference Between Quantum Annealing and Gate Models

A fundamental difference between these two approaches is that a gate model quantum computer requires problems to be expressed in terms of quantum gates, whereas the quantum annealing computer requires problems to be expressed in terms of operations research problems. That is one way to understand the difference between the two types of quantum computers.

What Are the Benefits of Quantum Annealer?

Once again and without treading over old ground, quantum annealing makes it possible to solve certain problems of huge complexity by designing the problem so that when the computer reaches its minimum energy state, it will be able to solve it.

IMPORTANCE OF QUBO MODELLING

An optimization technique known as QUBO (Quadratic Unconstrained Binary Optimization) is used in quantum computing, machine learning (ML), and optimization to solve complex optimization problems. The importance of QUBO models lies in their ability to represent complex optimization problems using binary variables, making translation into quantum computer language easier.

The importance of QUBO modelling can be attributed to several factors:

QUBO modelling is particularly useful for solving complex optimization problems. Various types of problems can be modelled using it, including scheduling, logistics, and finance, among others.

Another area where QUBO can benefit is quantum computing, as it allows it to tackle problems that classic computers would find impossible or extremely difficult.

Additionally, QUBO modelling is useful for feature selection in ML. ML models can be trained by identifying the most important features in a dataset.

Finally, when binary variables are used in QUBO modelling, the complexity of the optimization problem is reduced, allowing classical or quantum computing techniques to be used to solve the optimization problem.

How has Quantum Annealing Been Used in the Past?

To answer this question in part, we need to go back to the work of D-Wave, a company that has the honor of being the first in the world to sell computers that incorporated quantum effects into their operation.

D-Wave announced the first commercial quantum annealer on the market in 2011 with the name D-Wave One, which was described in a *Nature* paper. In terms of processor chipsets, the company claimed at the time this system had 128 qubits. A bit later in the same year, Lockheed Martin Corporation entered into an agreement with D-Wave to purchase a D-Wave One system.

According to a 2013 announcement, Google, NASA Ames and the non-profit Universities Space Research Association purchased an adiabatic quantum computer from D-Wave Systems.

A year later, and as part of its commitment to solving real-world problems with quantum hardware, D-Wave announced a new quantum applications ecosystem with computational finance firm 1QB Information Technologies (1QBit) and cancer research group DNA-SEQ.

What are the Future Prospects of Quantum Annealers?

Unlike traditional quantum computers, D-Wave had a different architecture in the past to most quantum computing companies but made an announcement at Qubits 2021 that the company was working on its first universal quantum computers that can run Shor's algorithm and other gate-model algorithms like QAOA and VQE. The business already has a strong base of Intellectual Property relevant to gate model quantum computing and it was seen as a natural next step within the organization.

April 2023 saw D-Wave publish results of one of the largest programmable quantum simulation ever reported. For the first time, a computation using more than 5,000 qubits in the D-Wave Advantage quantum computer showed coherent quantum dynamics being faster than classical dynamics in a programmable 3D spin glass, an intractable optimization problem.

Scientists from D-Wave and Boston University collaborated to publish the paper, entitled *"Quantum critical dynamics in a 5,000-qubit programmable spin glass,"* in *Nature*.

17.Secure Implementation of Post-Quantum Crypto in The Spotlight

by Marc Witteman
https://semiengineering.com/secure-implementation-of-post-quantum-crypto-in-the-spotlight/

The US-based NIST body takes a leading role in the migration to Post-Quantum Crypto (PQC). After a multi-year selection process, in 2022 they preliminarily identified a number of Post Quantum algorithms, which were recommended to replace the current public key algorithms (RSA, ECC). While the process of scrutiny is still ongoing, they now took another important step by putting emphasis on implementation security. Although the design of new algorithms comes first, this only makes sense if they can be securely implemented.

With implementation security we focus on two classes of Sensitive Security Parameters: Public Security Parameters, data that needs integrity (can't be modified), and Critical Security Parameters, which is data that also needs confidentiality (secrecy). In the protection of Sensitive Security Parameters we focus on the prevention of leakage of the Critical Security Parameters through Side Channel Analysis, and the robustness of all Sensitive Security Parameters against Fault Injection.

NIST hosted the first session about Side Channel Analysis (SCA) of PQC implementations on April 4. The second session on Fault Injection is planned for May 5. The SCA session was given by Professor Saarinen, who is also cryptography architect at PQShield, a pioneer in PQC implementation. Here's our review of the session focused on Side Channel Analysis.

The speaker recognized that protection against SCA is more challenging for PQC than for legacy crypto. Secure implementation requires the design of dozens of new 'gadgets,' which are implementations of cryptographic functionality that have built-in SCA protection. But, even before that, developers should consider time-constant program code. This is needed to prevent breaches when secret information can be derived by looking at the execution time of a process. However, it is a common misunderstanding that all crypto code needs to be time-constant. This requirement only applies to the handling of Critical Security Parameters. For instance, several PQC algorithms include a mechanism that is called 'Rejection Sampling,' which repeats an algorithm step until its results satisfy specific criteria. As long as these results cannot be traced back to key material, it is argued that this is not a problem.

Although leakage can ultimately lead to key retrieval, it is commonly acknowledged that security testing does not necessarily have to prove that keys can be extracted. One can even argue that by focusing on leakage it may only be possible to prevent future attacks that would exploit such leakage. The ISO 17825 standard provides a test procedure that evaluates leakage and includes a threshold for acceptable leakage levels.

It is very helpful that NIST stresses the importance of security implementation testing. As one of the few security labs that understand implementation security for PQC, Riscure is keen to help developers who seek assurance for their products. We look forward to the next presentation on the topic of Fault Injection.

18.The post-quantum cryptography conundrum

by Greg Hedges
https://www.cio.com/article/475040/the-post-quantum-cryptography-conundrum.html

Businesses in every industry may experience new threats when bad actors acquire access to cryptanalytically-relevant quantum computers, but they can start defending themselves now.

Business leaders may have heard of quantum computing, but many are not yet aware of its incipient threat to cryptography and cryptocurrency. When these machines reach a sufficient level of performance, they will be able to easily factor prime numbers, which poses a threat to RSA. Only a few realize that the time to prepare for the conundrum of post-quantum risk is now.

In quantum computing, the zeroes and ones underlying classical computing are replaced by quantum bits (qubits). These are made of subatomic particles. They produce complex computations exponentially faster than classical computing's ones and zeroes.

Quantum's risks

One great risk related to quantum computing is the belief that its capabilities will remain out of reach for a long time, yet some pundits have been remarking for 30 years now that the quantum threat is 30 years away.

As of this writing, about three dozen quantum computers are already available in the cloud. While these machines pose no risk, national governments, global authorities, and experts regard the availability of a **cryptanalytically-relevant quantum computer** (CRQC) as an imminent threat.

Cryptocurrency and the blockchain

Imagine a bad actor possessing a CRQC and downloading a blockchain. They'll reverse all transactions where addresses are reused to obtain those wallets' private keys. Then, they'll steal all the cryptocurrency those wallets contain.

The elliptic curve cryptography used in blockchain is more susceptible to quantum computing attacks than RSA encryption used to protect sensitive data in motion such as credit card transactions. Based on two well-known papers, **2,500 error-corrected qubits** will be needed to crack some blockchains, while over **4,000 such qubits** will be needed to attack 2048-bit RSA. Newer, **quantum-resistant approaches for blockchains are emerging**, but it's still early days. Businesses that make use of the blockchain will want to monitor developments in quantum-resistant approaches.

Sensitive data

Public key encryption techniques – used today for email, financial transactions, and other sensitive communications – will be broken when a CRQC becomes available to bad actors.

This is not only a threat to future transactions but also already a threat to data. Nation states and other bad actors are already stealing encrypted data, anticipating capabilities to decrypt these assets to be-

come available within a few years.

Mosca's Theorem adds the years it could take an organization to migrate to **post-quantum cryptography (PQC)** to the years the data must be kept safe. For industries like healthcare or insurance, the shelf life of sensitive data is a lifetime. This total is almost always longer than estimates of a CRQC arriving, which means the secrets will be exposed. to the years the data must be kept safe. For industries like healthcare or insurance, the shelf life of sensitive data is a lifetime.

Now is the time to identify sensitive data in preparation for applying new algorithms and ciphers as soon as they're available.

Regulation

In May 2022, the White House released a **memorandum** to describe the U.S. government's expectations of all federal agencies: "When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions… To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

It's likely that other authorities will adopt similar requirements for the industries they regulate.

Meanwhile, the United States Department of Commerce's **National Institute of Standards and Technology (NIST)** is conducting global efforts to standardize PQC algorithms. They'll publish the standard in twelve to eighteen months.

Standardization will be the inflection point at which most individuals – including board members – take interest in the conundrum of post-quantum risk. When NIST announces the standards, board members and other stakeholders will want to know how crypto-agile their organizations are – but by then, we believe it will be too late.

Crypto-agility

"**Crypto-agility** measures how well your company can adapt to new cryptographic primitives and algorithms without making disruptive changes. Every company will need to achieve this bragging right as soon as possible to avoid the coming quantum computing cryptographic apocalypse. This includes a combination of auditing where you are on the journey and then actually taking action."

Crypto-agility should be the goal of every organization, but how many of them can pass a crypto-agility assessment today? The answer is: no organization today is fully crypto-agile. The good news? All organizations can make progress toward crypto-agility, starting from wherever they are.

Why act now?

For the first time ever, security professionals enjoy the luxury of knowing about a "**zero day**" before it happens. They don't have to be caught unaware.

Among the reasons to work toward crypto-agility now:

- In anticipation of CRQC availability, bad actors are already storing data.
- Transition to PQC will take considerable time.

- NIST has already identified one finalist PQC algorithm.
- Businesses and individuals alike will experience theft from compromised blockchains.
- Even as the world awaits PQC standards, guidance is available and businesses can take action to prepare.

Approach

Some security leaders are taking steps to become crypto-agile by:

- Starting with a post-quantum cryptography agility assessment to determine their current state and identify gaps.
- Determining where their most highly valued and sensitive data is stored, and how it moves between systems, functions, and enterprises.
- Inventorying ciphers they use today. This activity identifies which ciphers must migrate to PQC. With this action, organizations begin to understand how adapting to PQC will impact the organization and its current systems.
- Assessing proprietary software. Some custom code may incorporate security features in an inflexible way that would need rewriting. Geometry Labs has released a "lattice-algebra" library to bring a high-performance cryptographic library to developers interested in using post-quantum cryptography in blockchain and other applications and joined us recently for a Post-Quantum World podcast on the topic. Evaluating the crypto-agility of providers whose platforms, infrastructure, and software as a service (PaaS, IaaS, SaaS) are in use.

Businesses of any industry may experience new threats when bad actors acquire CRQCs, but they can start defending themselves now. Keep up to date with quantum threats – and opportunities – with ***The Post-Quantum World*** podcast.

19.FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology

by The White House
https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

Today, the Biden-Harris Administration released the United States Government's National Standards Strategy for Critical and Emerging Technology (Strategy), which will strengthen both the United States' foundation to safeguard American consumers' technology and U.S. leadership and competitiveness in international standards development.

Standards are the guidelines used to ensure the technology Americans routinely rely on is universally

safe and interoperable. This Strategy will renew the United States' rules-based approach to standards development. It also will emphasize the Federal Government's support for international standards for critical and emerging technologies (CETs), which will help accelerate standards efforts led by the private sector to facilitate global markets, contribute to interoperability, and promote U.S. competitiveness and innovation.

The Strategy focuses on four key objectives that will prioritize CET standards development:

- **Investment:** Technological contributions that flow from research and development are the driving force behind new standards. The Strategy will bolster investment in pre-standardization research to promote innovation, cutting-edge science, and translational research to drive U.S. leadership in international standards development. The Administration is also calling on the private sector, universities, and research institutions to make long-term investments in standards development.

- **Participation:** Private sector and academic innovation fuels effective standards development, which is why it's imperative that the United States to work closely with industry and the research community to remain ahead of the curve. The U.S. Government will engage with a broad range of private sector, academic, and other key stakeholders, including foreign partners, to address gaps and bolster U.S. participation in CET standards development activities.

- **Workforce:** The number of standards organizations has grown rapidly over the past decade, particularly with respect to CETs, but the U.S. standards workforce has not kept pace. The U.S. Government will invest in educating and training stakeholders — including academia, industry, small- and medium-sized companies, and members of civil society — to more effectively contribute to technical standards development.

- **Integrity and Inclusivity:** It is essential for the United States to ensure the standards development process is technically sound, independent, and responsive to broadly shared market and societal needs. The U.S. Government will harness the support of like-minded allies and partners around the world to promote the integrity of the international standards system to ensure that international standards are established on the basis of technical merit through fair processes that will promote broad participation from countries across the world and build inclusive growth for all.

Putting the Strategy into Practice

The U.S. private sector leads standards activities globally, through standard development organizations (SDOs), to respond to market demand, with substantial contributions from the U.S. Government, academia, and civil society groups. The American National Standards Institute (ANSI) coordinates the U.S. private sector standards activities, while the National Institute of Standards and Technology (NIST) coordinates Federal Government engagement in standards activities. Industry associations, consortia, and other private sector groups work together within this system to develop standards to solve specific challenges. To date, this approach has fostered an effective and innovative standards system that has supercharged economic growth and worked for people of all nations.

The CHIPS and Science Act of 2022 (Pub. L. 117–167) provided $52.7 billion for American semiconductor research, development, manufacturing, and workforce development. The legislation also codifies NIST's role in leading information exchange and coordination among Federal agencies and communication from the Federal Government to the U.S. private sector. This engagement, coupled with the CHIPS and Science Act's investments in pre-standardization research, will drive U.S. influence and leadership in international standards development. NIST provides a portal with resources and standards information to government, academia, and the public; updates on the U.S. Government's implementation efforts for the Strategy will also be posted to that portal.

The United States Government has already made significant commitments to leading and coordinating international efforts outlined in the Strategy. The United States has joined like-minded partners in the International Standards Cooperation Network, which serves as a mechanism to connect government stakeholders with international counterparts for inter-governmental cooperation. Additionally, the U.S.-EU Trade and Technology Council launched a Strategic Standardization Information mechanism to enable transatlantic information sharing.

Many U.S. Government agencies have already demonstrated their commitment to the Strategy through their actions and partnerships. Examples include:

- The National Science Foundation has updated its proposal and award policies and procedures to incentivize participation in standards development activities.

- The Department of State, NIST, the Department of Commerce, the Federal Communications Commission (FCC), the National Security Agency (NSA), the Office of the U.S. Trade Representative, USAID and other agencies engage in multilateral fora, such as the International Telecommunication Union, the Quad, the U.S.-EU Trade and Technology Council, the G7, and the Asia-Pacific Economic Cooperation, to share information on standards and CETs.

- The National Telecommunications and Information Administration (NTIA) administers the Public Wireless Supply Chain Innovation Fund, a $1.5 billion grant program funded by the CHIPS and Science Act of 2022 that aims to catalyze the research, development, and adoption of open, interoperable, and standards-based networks.

- The Department of Defense engages with ANSI and the private sector in collaborative standards activities such as Global Supply Chain Security for Microelectronics and the Additive Manufacturing Standards Roadmap, as well as with the Alliance for Telecommunications Industry Solutions and the 3rd Generation Partnership Project (3GPP).

- The United States Agency for International Development and ANSI work together through a public-private partnership to support the capacity of developing countries in areas of standards development, conformity assessment, and private sector engagement.

- The Environmental Protection Agency SmartWay program works closely with the International Organization for Standardization (ISO) to standardize greenhouse gas accounting for freight and passenger transportation, providing a global framework for credible, accurate calculation and evaluation of transportation-related climate pollutants.

- NTIA, NIST, and the FCC coordinate U.S. Government participation in 3GPP and work with the Alliance for Telecommunications Industry Solutions to ensure participation by international standards delegates at North American-hosted 3GPP meetings.

- The FCC's newly established Office of International Affairs is managing efforts across the FCC to ensure expert participation in international standards activities, such as 3GPP and the Internet Engineering Task Force, in order to promote U.S. leadership in 5G and other next-generation technologies.

- The Department of Transportation supports development of voluntary consensus technical standards via multiple cooperative efforts with U.S.-domiciled and international SDOs.

- The U.S. Department of Energy (DOE), though partnerships with the private sector and the contributions of technical experts at DOE and its 17 National Laboratories, contributes to standards efforts in multiple areas ranging from hydrogen and energy storage to biotechnology and high-performance computing.

- The Department of the Treasury's Office of Financial Research leads and contributes to financial data standards development work for digital identity, digital assets, and distributed ledger technology in ISO and ANSI.

The actions laid out in the Strategy align with principles set forth in the National Security Strategy, the National Cybersecurity Strategy, and ANSI's United States Standards Strategy, and will not only protect the integrity of standards development, but will ensure the long-term success of the United States' innovation.

20.Germany Announces 3 Billion Euro Action Plan For a Universal Quantum Computer

by Matt Swayne
https://thequantuminsider.com/2023/05/03/germany-announces-3-billion-euro-action-plan-for-a-universal-quantum-computer/

Germany's action plan for quantum technologies is set to invest a total of 3 billion euros in the development of a universal quantum computer by 2026, according to the federal government's "action concept for quantum technologies," according to German media.The aim is for Germany to catch up with international development in the US and China. Of the 3 billion euros, the lead research ministry will receive 1.37 billion euros of the funds, with an additional 800 million euros in the budgets of state-financed research institutes. The cabinet is expected to launch the concept by the end of April.

Federal Research Minister Bettina Stark-Watzinger said that quantum technology is crucial for Germany's technological sovereignty. The aim is for the development of a quantum computer to trigger further investment in the industry.

"With the action plan, we in Germany want to secure a place at the top of the world in quantum technologies and our technological sovereignty," said Stark-Watzinger.

The planned German quantum computer should have a capacity of at least 100 qubits by 2026 and be expanded to 500 qubits "in the medium term". This is a smaller capacity compared to, for example, IBM in 2022. However, with a total of around three billion euros in funding, German technology reporters suggest that that Germany is positioning itself at the top end in a European comparison.

More Than A Quantum Computer

The initiative is more than just about Germany's capacity to build a quantum computer, but it's also a commitment to build a quantum ecosystem and a quantum industry. The plan lists five goals:

- To secure and expand Germany's innovative power and technological sovereignty in quantum technologies.
- To work towards the development and production of marketable products.
- To contribute to addressing societal challenges in climate research, energy, health, mobility, and security with quantum technologies.

- To educate and attract skilled workers and develop Germany as an attractive employment location for quantum technologies.
- To introduce people to quantum technologies, convey the opportunities, and show the impacts.To ensure a coordinated, joint approach by the federal government.

Quantum computers are considered to be the future key technology as they can perform calculations in seconds, which would take powerful conventional computers years. While traditional computers pass information in bits, quantum computers use qubits, which can take any value between zero and one, making them more powerful.

According to Stark-Watzinger, eventually quantum computers could help perform tasks that include simulating new drug compounds, secure communication, and innovative sensors for detecting contaminated ordnance or navigation without satellite support.

Germany's economy would also benefit from software development, component construction and the use of quantum technology, says Wilhelm-Mauch.

21.Australia Announces National Quantum Strategy

by Matt Swayne
https://thequantuminsider.com/2023/05/03/australia-announces-national-quantum-strategy/

The Australian Government released the country's first National Quantum Strategy that sets a long-term vision for Australia to take advantage of the opportunities in quantum, according to a statement from the Department of Industry, Science and Resorces.

According to a statement, Australia has been at the forefront of quantum science and technology for more than 2 decades. We have world-class research institutions, talented scientists and engineers and a vibrant start-up ecosystem. The strategy outlines how we will seize our quantum future and remain a global leader.

The strategy will serve to guide collaboration between research pioneers, industry partners, start-ups and the government, Ed Husic, Minister for Industry and Science said in a statement. The collaborations could create a new era of practical quantum tech, he added.

"In time, quantum computing will unleash incredible computing power that can phenomenally outperform traditional computing," said Husic. "By pairing a National Quantum Strategy with the National Reconstruction Fund we're aiming to turn Australia into a global technology leader, building stronger industry and creating jobs for the future."

The strategy identifies five priority areas: investing in research and development and commercialisation, securing infrastructure and materials, growing a skilled workforce, supporting national interests and promoting a trusted, ethical, inclusive ecosystem.

Considering some use case priorities, the statement reports that quantum technologies could help solve some of the biggest challenges:

- Cutting the time and cost of developing new medicines

- Helping the transition to net zero with more efficient battery storage
- Safeguarding cyber infrastructure

The payoff is significant. According to the statement, quantum industries could create 19,400 direct jobs, with $5.9 billion of revenue by 2045.

“I can’t emphasise this enough, quantum technologies will be truly transformative,” said Husic. “We are already seeing how quantum sensing equipment is making a huge difference for industry.”

Australia’s plan is based on extensive consultation across industry, researchers and the community led by Australia’s Chief Scientist Dr Cathy Foley and with guidance from the National Quantum Advisory Committee.

According to Foley, the plan recognizes Australia’s pioneering role in quantum research as a strength.

“Australia has had its finger on the quantum pulse since Professors RQ Twiss and AG Little published the first paper on time-correlated photons in 1959,” Foley writes in her statement. “Since then, and especially in the past 25 years, we’ve made significant research investment, resulting in an emerging Australian quantum industry that is destined to have a significant impact on all of our lives.”

She adds that it will be critical to connect that research with the nation’s entrepreneurial spirit.

“Australia is well positioned to capitalise on the amazing research that is making its way out of the lab,” Foley writes. “Our entrepreneurial spirit is generating new start-ups and attracting major companies. This is our chance to grow a thriving deep-tech industry, built out of coordinated, long-term government investment and a critical mass of world-class Australian-trained quantum specialists. We are in the top handful of countries embarking on a quantum ambition. But we have to act now, as there is intense global attention on the promise of quantum.”

22.A Brief Overview of Quantum Computing in India

by James Dargan
https://thequantuminsider.com/2023/05/03/a-brief-overview-of-quantum-computing-in-india/

Research and development on quantum computing technology have been actively carried out in India for a number of years. In an effort to support the growth of India’s quantum computing, the government has established several initiatives to support its development.

India’s Government Position

One of the major initiatives is the Quantum Computing Applications Lab (QCAL), which was launched by the Ministry of Electronics and Information Technology (MeitY) in collaboration with AWS. QCAL aims to accelerate the adoption of quantum computing in India by providing access to quantum computers, tools, and resources to researchers and developers.

The National Mission on Quantum Technologies and Applications (NM-QTA) was launched in 2020 with the goal of creating a strong quantum technology ecosystem in India. Over the next few years, it will cost Rs. 8,000 crores ($ 1.2 billion) and be implemented by the Department of Science and Technology. Un-

der the Prime Minister's Science and Technology Innovation Advisory Council (PM-STIAC), Quantum Technologies & Applications is one of 9 missions of national importance. The program contributes to scientific research for India's sustainable development through the office of the Principal Scientific Advisor.

The Quantum Measurement and Control Laboratory (QuMaC) studies quantum phenomena in superconducting circuits. Nanofabricated electrical circuits are engineered to behave as quantized "artificial atoms."The two levels can be combined to form a quantum bit (qubit) that stores and processes information. Using these qubits, one can build powerful computing machines capable of solving certain mathematical problems exponentially faster. The Lab aims to develop and control such quantum systems by addressing the fundamental challenges.

Research

Several universities and research institutions in India are also actively involved in quantum computing research. A quantum computing centre at the Indian Institute of Science (IISc) in Bangalore focuses on quantum algorithms, quantum information theory, and quantum error correction.

Other institutions such as the Indian Institute of Technology (IIT) Madras and the Harish-Chandra Research Institute (HRI) in Allahabad also have active research programs in quantum computing.

Aside from research, India is also building a quantum computing workforce. Many Indian government programs are geared towards training students and researchers in quantum computing, including the National Mission for Quantum Frontier.

Private Sector

Large Indian corporations invested in quantum include information technology services and consulting company TCS — it offers a quantum computing internship program that has been offered by the company in partnership with IIT Tirupati.

Another is Infosys, which has launched 'Infosys Quantum Living Labs' for its clients who are interested in exploring quantum computing use cases.

Tel Aviv University has partnered with Wipro, a corporation that provides information technology, consulting and business process services, to strengthen Indo-Israeli scientific collaborations on quantum science and technology.

In order to speed up fundamental and applied research in quantum computing, Mphasis — an applied technology services company based in Bangalore — has partnered with IIT Madras to fund startups, develop talent, and provide scholarships.

HCL Technologies has collaborated with Sydney Quantum Academy. Through this partnership, the two hope to provide students with quantum technology education and R&D opportunities.

Smaller players are also in on the game too, as India is well represented here, with a handful of startups busy working on their own IP in quantum tech.

In addition to multidisciplinary optimization, BosonQ Psi develops quantum computing software solutions including computational fluid dynamics, computational structural dynamics, computational heat transfer, and computational aeroacoustics. Founded in 2020 and based in Bhilai, Chhattisgarh, the company's solutions are set to help in the development of a wide range of applications that include aerospace, automotive, power generation, chemical manufacturing, polymer processing, petroleum explo-

ration, medicine, meteorology, and astrophysics.

A female-founded company, Qkrishi provides quantum models, algorithms and kernels for a wide range of industries. The Birla Institute of Management Technology has also partnered with them to create a first-of-its-kind Quantum Computing course that integrates business and technical elements.

As a quantum cyber-security company based in Bangalore, QuNu Labs was founded in 2016. A basic QKD system based on Differential Phase Shift Protocol is their first product, following four years of initial research and incubation at IIT Madras.

Key People for India's Quantum Computing

With a huge population and many elite technical universities to choose from, it was difficult to "pick" certain individuals who are influencing quantum computing in India, but we managed to select two who are notable in the sector.

Although not directly working in quantum, Ashutosh Sharma, Secretary of the Department of Science and Technology, Government of India, has been a strong advocate for quantum computing research in the country. A chemical engineer by trade, Sharma completed his master's degree at Pennsylvania State University in 1984, before going on to earn his Ph.D. in Chemical Engineering at the University at Buffalo.

In 2021, Sharma said that in order for India to remain competitive and cooperate with its partners, the country must harness the potential of quantum technology and its applications.

Another important person who is pushing for India to take the lead in quantum technology is Ujjwal Sen. Sen has worked on several topics in quantum information theory, including quantum communication and quantum cryptography at the Harish-Chandra Research Institute in Allahabad and his main research interests are in quantum information and computation, as well as their interface with many-body physics.

Sen obtained his Ph.D. in Physics from the University of Gdansk, Poland, where he specialized in quantum information, quantum optics and the foundations of quantum mechanics.

Conclusion

Overall, India is taking significant steps towards establishing itself as a leading player in the global quantum computing industry. With the right support and investment, India has the potential to become a major hub for quantum computing research and development.

23.Understanding and Minimizing the Security Risks of the Quantum Revolution in Computing

by Julia Rabinovich
https://blog.checkpoint.com/security/understanding-and-minimizing-the-security-risks-of-the-quantum-revolution-in-computing/

Recently we covered the state of quantum computing and its potential societal benefits. Now we will

cover **the potential impact of quantum computing on cybersecurity** and how we at Check Point Software are innovating to ensure our customers receive the best security today and in the future.

Today's cybersecurity solutions utilize public key cryptography to achieve secure communication and data protection. Public key algorithms are employed to ensure confidentiality, authentication, and data integrity. The security of cryptographic operations, such as signing, encryption, and key exchange, is dependent on the security of public key algorithms – mostly on RSA, Diffie-Hellman, Elliptic Curve – which rely on mathematical problems involving discrete algorithms and integer factorization. The fact that classical computers are unable to solve these problems, and therefore unable to break these algorithms, reinforces the security of the majority of cryptographic systems used today.

Quantum computers operate on the principles of quantum mechanics, which allow them to manipulate and process information in ways that classical computers cannot. As a result, quantum computers have the potential to solve certain types of problems exponentially faster than classical computers.

Quantum Computing's Impact on Cybersecurity

Quantum computing's exponential performance advantage, combined with dedicated algorithms (like Shor's algorithm) focused on resolving specific cryptographic problems, could significantly reduce the computational time required for breaking any public key algorithm based on integer factorization and discrete log. Breaking public key algorithms enables the computer to extract the encryption key and therefore decrypt all data. Unfortunately, algorithms used today by all major networking protocols are public key based and therefore are vulnerable. Or put another way: quantum computing could effectively make it possible to break today's encryption.

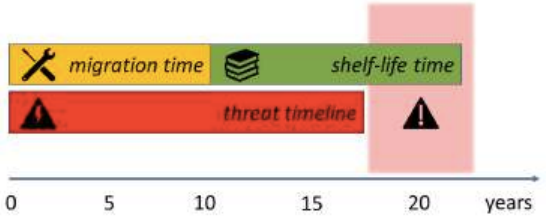
Encryption protects private and sensitive data. Every time a consumer makes a purchase through an app or a website, encryption is used to protect their financial and personal information. Encryption also protects medical data, company intellectual property and so much more.

So far, this breaking algorithm operation cannot be performed with today's quantum computers. It will require a cryptographically relevant quantum computer (**CRQC**) to put the security of the Internet's data transmissions via TLS, SSH, FTP and VPN networking protocols at risk.

Timing Question

The strongest quantum computer we have today is from IBM. It has 433 qubits. Researchers expect a CRQC will require approximately 8K qubits to decrypt encrypted data. The industry expectation is that commercial CRQC will be available around 2030.

However, there is another risk that needs to be taken into consideration. The "harvest today, decrypt later" attack assumes that some elements may record encrypted data communications today, store it and decrypt it later with CRQC to extract sensitive data. The following famous figure, created first by Dr. Michele Mosca and known as Mosca's Theorem, illustrates timelines associated with the risk of this attack:



Given that CRQC will likely be available in less than 10 years and that in most cases data shelf-life time is 7-10 years, the industry should migrate to quantum safe solutions ASAP.

How Can We Protect Sensitive Data?

Addressing this security issue requires a consolidated effort between government, research and cyber-security organizations worldwide.

To protect against this threat, the National Institute of Standards and Technology (NIST) established a Post-Quantum Cryptography Standardization Forum to unite the crypto experts from different countries, private, government and academic organizations. The forum aims to define and standardize new algorithms that are "quantum safe" (resistant against quantum computer attacks). The new algorithms should gradually replace the non-quantum safe algorithms used today by the industry.

Lately there has been significant progress in the work led by NIST. With the completion of the third round of quantum safe algorithm validations, the Forum came to conclusion that they are ready to announce the first four algorithms that are quantum safe.

Quantum safe solutions

What is the quantum safe solution? It's a solution that cannot be broken using CRQC. Such solutions can be built in at least two ways:

- **Software upgrade approach**: the vulnerable public key algorithms are completely replaced with the quantum safe ones. This approach addresses all spheres where the vulnerable algorithms are used – identification and authentication, confidentiality and data integrity. The main risk associated with this approach is related to reliability of the new algorithms from the security perspective.

- **Quantum key distribution (QKD) approach**: the encryption key produced by one of the existing and potentially vulnerable public key algorithms is enhanced with additional key material or fully replaced with an external key. The additional key material or external key is generated independently and delivered over a dedicated quantum channel. The data transmission operates on the principles of quantum mechanics. This QKD solution is relatively new and still have certain physical limitations. This approach addresses only the issue of confidentiality in the data networking scenarios (e.g. VPN).

Of note, the National Security Agency (NSA) in the USA, the National Cyber Security Centre (NCSC) in the UK, and the Federal Office of Information Security (BSI) in Germany have clearly stated their recommendation to follow the software upgrade approach as the safest and most reliable approach.

Recent Developments

In the past year and a half, government agencies have started to publish guidelines and recommendations in the push for post-quantum encryption.

- **January '22**: the White House published "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," that directed the NSA to publish updated guidelines related to the transition to quantum safe computing, including timelines.

- **March '22**: following the White House directives, the NSA published an updated CNSA 1.0 (CNSS-15) specification, naming recommended algorithms to be used during the transition period.

- **July '22**: the NIST Post Quantum Cryptography Standardization committee announced four Post-Quantum Cryptography candidates for cybersecurity in the quantum computer era.

- **September '22**: the NSA released the Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems, the first explicit requirements declaring quantum safe algorithms for all functional areas as well as migration and enforcement timelines.

- **January '23:** Germany's BSI published Security Requirements with guidelines and recommendations on algorithms and key sizes to be used for the transition period.

What Should Happen Now?

All software (and impacted hardware) vendors should begin providing solutions in the data communication and networking areas to ensure compliancy to the latest security recommendations for the migration period, while the non-quantum safe algorithms are still in use.

1. All software (and impacted hardware) vendors providing solutions in the data communication and networking areas, need to start mapping all services and solutions that are using not quantum safe algorithms and plan the migration process to the quantum safe algorithms.

2. The standards for the new algorithms replacing classic public key algorithms should be published by relevant international standardization organizations.

3. All protocols and digital entities (like certificates) should enable hybrid operational mode. This means that when old algorithms will coexist with the new ones, they should be updated to enable smooth migration to the quantum safe solutions.

4. All commonly used open source libraries like openSSL and openVPN should be updated by the community, adding support for the new algorithms.

5. All companies relying on data protection and exchange solutions should identify all impacted products and ensure that software vendors providing these solutions are aligned with the industry migration roadmap drawn by CNSA 2.0 and other regulations.

Check Point's Transition Plan to Quantum Safe Computing

As a preparation for the quantum computing era, Check Point is taking concrete steps to ensure customers will remain secure and their data private:

- As an immediate step, Check Point published a knowledge base article (sk178705) outlining the steps customer can take to implement NSA recommendations for using stronger keys for site-to-site encryption.

- Upon demand, Check Point Security Gateways will be ready for proof-of-concept implementation of quantum key distribution (QKD) deployments by allowing an external system to provide symmetric encryption keys. Research suggests that QKD will be able to detect the presences of an eavesdropper, which is not possible in standard cryptography.

- Additionally, Check Point will support Kyber, a post quantum computing (PQC) safe algorithm by July 2024, allowing customers to implement a backward compatible, quantum safe, site-to-site IPsec encryption.

We live in an exciting time of innovation. As researchers make progress toward realizing the benefits of

quantum computing, at Check Point Software we remain dedicated to ensuring that our customers have the best security to protect them against advanced cyber attacks. We will continue to share updates as the field progresses.

24.The cloud revolution: How Cloud HSMs are redefining enterprise cryptography

by BFSI Network
https://bfsi.eletsonline.com/the-cloud-revolution-how-cloud-hsms-are-redefining-enterprise-cryptography/

HSMs are used by some of the biggest organisations around. However, cloud solutions have provided a much larger number of organisations with the ability to swiftly deploy enterprise cryptography in a cost-effective manner, shares **Ruchin Kumar**, Vice President – South Asia, Futurex, in an exclusive interaction with Srajan Agarwal of **Elets News Network (ENN).**

Which sectors have taken lead in the adoption of General Purpose and Cloud Payment HSMs? Where do you see maximum growth in demand for your cloud payment and general-purpose HSMs to come from in 2023?

Where there's a need to protect sensitive data, there's a need for HSMs. Some of the biggest industries that come to mind are payments, retail, government and defense, and healthcare. Where payment data is involved, you'll find the need for payment HSMs, either on-premises or in the cloud. Where personal identifiable information (PII) is dealt with, you'll see more demand for general-purpose HSMs. Of course, general-purpose HSMs do more than encrypt PII. They can be used to encrypt databases, files, and applications, and can generate and manage encryption keys, forming the basis for public key infrastructure (PKI), certificate authority (CA), Blockchain products and IOT. General Purpose HSMs also plays a great role in securing the root key of trust used in digital signing of messages/files/transactions to ensure integrity and non-repudiation.

More and more companies are migrating critical infrastructure to the cloud. They benefit from the OpEx (versus CapEx) financial model and on-demand scalability. However, there is an increasing need for cloud cryptography platforms with a truly global reach that complies with data localisation requirements. Our global cloud offering is one way we really stand out from other cryptography providers, and has been a source of growing demand among our customer base.

What are the primary obstacles and opportunities for HSM adoption in India? How do you intend to capitalise on opportunities and effectively resolve challenges?

HSMs are used by some of the biggest organisations around. However, cloud solutions have provided a much larger number of organisations with the ability to swiftly deploy enterprise cryptography in a cost-effective manner. Futurex's local Indian data centers deliver low latency and high availability to our customers and partners in the region. The Futurex cloud makes it so that organisations don't have to worry about data localisation regulations, either.

Which industries, in your opinion, have taken the lead in embracing Cloud Payment HSMs? And how does your company make HSMs inexpensive to fintechs and small payment organisations?

India is home to a large number of fintechs, with more emerging all the time. We've noticed that our

cloud solutions lower the barrier to entry among organisations like these. The VirtuCrypt cloud offers a pay-as-you-go OpEx model instead of the upfront expense of a CapEx model. Organisations have the freedom to begin deploying infrastructure in the cloud and scale up or down according to need. Above all, Futurex HSM expert team helps in typical integration and management issues.

What recommendations do you have for CIOs/CTOs/CISOs of fin-tech companies/payment organisations aiming to instil customer trust in digital transactions?

More encryption is always better, and strong encryption is best. Hardware-based encryption—whether deployed on-premises or in the cloud—is the best way of achieving both of these goals at once. Hardware-based encryption is where cryptographic processes are performed inside of a temper resistant FIPS certified physically secure boundary; likewise, cryptographic keys are stored in dedicated hardware components that are physically secure.

Using hardware-based encryption solutions validated under international standards like PCI HSM is a great way to maintain trust in your organisation's security. PCI validation entails strict compliance and serves as a badge of trust among customers and partners.

At the end of the day, business depends on trust, and trust depends on encryption security of encryption keys responsible for doing encryption. That's why it's important to find an encryption and key management provider that is likewise trusted across the industry.

With cybercrime on the rise, what role do you see for tokenisation and application encryption technology in beefing up cyber security?

Tokenisation is where data—such as payment card information—is substituted with randomised strings or "tokens" and stored in encrypted form. This makes it so that attackers can't retrieve the clear-text data. However, tokenisation can entail the use of storage systems called "token vaults," where tokens are held. Token vaults can entail their own attack vectors, which is why Futurex uses "vaultless tokenisation" to further secure the tokenisation process. Deploying a vaultless tokenisation solution helps protect payment data with fewer points of attack and better security.

Application encryption is crucial for most organisations. Most organisations deal with multiple applications, each of which may use thousands of encryption keys. To avoid cryptographic sprawl and the resulting vulnerabilities, organisations are well-advised to consider deploying a robust key management solution. Using good key management helps define and automate how your encryption keys are created, distributed, stored, rotated, and destroyed. Not only does it reduce manual effort, it tightens security and opens the door to new cryptographic possibilities within your organisation.

25.Biden to private sector: Cybersecurity is your responsibility—not the user's

by Brandon Kirk Williams
https://thebulletin.org/2023/05/biden-to-private-sector-cybersecurity-is-your-responsibility-not-the-users/

The Biden administration's recently-released National Cyber Strategy proposes a new social contract that places the responsibility of protecting the nation's cybersecurity on the private sector, not individual users. The novel model for national cyber resilience, which overturns decades of cybersecurity practice,

is the result of an impending avalanche of disruptive technological threats that will eclipse the ability of everyday citizens and small businesses to protect data. No longer can the country rely on a model where private sector vendors and suppliers push security onto users. The National Cyber Strategy pledges to use government power to realign incentives and shape markets—by using carrots of government funding and sticks of regulation—to forge a new social contract for cybersecurity at a transitional moment.

Unlike previous such strategies, the new National Cyber Strategy rebalances responsibility to generate a new social contract for a resilient national cybersecurity to counter threats from malicious nations and emerging technology. Only the private sector can embed security-first product development to protect the country's information architecture from the converging threats of the modernizing internet, quantum computing, and the hyper-connected Internet of Things (IoT), a network of physical objects, or "things," connected to the internet that ranges from pacemakers to home ovens. In its call for new principles for cyber resilience, the document overturns decades of accepted practice for the private sector and constraints on government. It moves beyond rhetoric to declare that government must utilize its authorities to correct misaligned incentives that will jeopardize a flourishing digital ecosystem—a striking proposition.

Now-retired National Cyber Director Chris Inglis coordinated the writing of the Biden administration's document. This is the first such document prepared by a national cyber director, and this version stands above all previous cyber strategies. Inglis and his team structured the document around five pillars, two of which—"Shape Market Forces to Drive Security and Resilience" and "Invest in a Resilient Future"—are most remarkable for outlining a new direction for cyber. The other pillars contain noteworthy changes, but nothing near the ruptures of those two, known as pillars three and four.

Pillar three. In this section, titled "**Shape Market Forces to Drive Security and Resilience**," the document unambiguously states that current market dynamics have failed to reduce threats and incentivize vendors and suppliers to put secure-by-design principles in the foreground when rolling out products. Stewards of data, the strategy insists, bear the responsibility for safeguarding information against malicious actors. The private sector owns and operates the majority of the nation's internet; risk mitigation for data theft, poor design, and vulnerabilities therefore should fall on industry. But until now, industry has possessed little incentive to ensure that a foundation of security is firmly established, even were it to slow the growth of the Internet of Things or a software release.

The result is a digital ecosystem that's ill prepared for a future of metastasizing threats.

The Biden cyber team, however, did not pen an anti-capitalist screed. Pillar three emphasizes that "market forces remain the first, best route to agile and effective innovation," but it acknowledges that jockeying for market share has come at the expense of the United States' economy and national security. The solution? Guiding the market via incentives and regulation to guarantee that security remains at the heart of innovation—before technological threats compound and vandalize the country's digital ecosystem.

The Biden administration's threat perception is shaped by the systemic risks posed by an explosion of Internet of Things vulnerabilities and by software that neglects basic best security practices. From households to critical infrastructure to health devices, little in the United States will go untouched by the Internet of Things in coming decades. Proliferating Internet of Things devices multiply the attack surfaces that threat actors can target for data exfiltration, hijacking for botnets, or to surveil users. Dell projects that 41.6 million internet-connected devices will be operational in 2025, and usage estimates climbs year-after-year. Internet of Things vendors often elevate deployment over security. Everyday consumers possess scant ability to manage upgrades or have full knowledge of limited liability that is often buried in contracts. Similarly, software designers and vendors are encouraged to rush products to market without safety assurances for users. The lack of uniform testing protocols, or clarity on third-party inputs, leaves users susceptible to risk; and little evidence exists that the market will correct for negligence in software or Internet of Things.

Pillar three endorses a stronger federal presence and regulation to overcome the lax oversight that allowed vulnerabilities to flourish at the expense of protecting users. The administration's prescriptions include transparent labeling for internet-connected devices, updated government procurement policies, and software liability legislation. The latter is most far-reaching but would also provide an option for companies to adopt—a software safe harbor—that establishes best design and development practices. Utilizing a software safe harbor would shield companies from legal action, provide users with the knowledge of vendors that meet standards, and steer innovation. Instead of depicting regulation as a burden that stifles the market, the strategy's authors insist that government oversight nourishes a healthy innovation ecosystem. In this sense, the state is exercising its power to realign the mismatch between public and private interests while also providing users with the agency to influence industry.

Pillar four. "**Invest in a Resilient Future**" envisions how government can leverage federal spending to prepare for a transition to a new era of both technological threat and opportunities. This part addresses the gap between public and private capital that leaves the country vulnerable as it anticipates challenges to the foundation of the internet, quantum technologies, and nation-wide electrification. Pillar four identifies the necessity of federal initiatives to ensure citizens can rely on secure infrastructure—ranging from information architectures to the electrical grid—that the private sector will not fund, because only the government can fill the gap.

The fourth pillar identifies three foundational threats that require federal investment: the internet's evolving network ecosystem, post-quantum encryption, and a resilient-by-design electrical grid. Although the private sector owns the bulk of the internet, modernizing governmental networks can create momentum to alter the nation's internet. The baseline domains and protocols undergirding the internet are currently updating to a more secure space with fewer attack surfaces. Internet Protocol version 6 (IPv6) is replacing its legacy predecessor version 4. (Internet protocols govern how data is transmitted and received across networks.) The National Security Agency's guidance for mitigating threat in the transition from Internet Protocol version 4 to Internet Protocol version 6 stresses that the former is inadequate for the expanding number of devices that will require connectivity.

The latest cyber strategy's authors also adopt a medium-term view on the future of post-quantum cryptography. Recognizing the vulnerabilities in the transition to quantum computing, pillar four pledges that government will accelerate its funding of basic research and development of cybersecurity solutions. A fully operational quantum computer that can compromise standard RSA encryption (algorithm for secure data transition) could be 10 years away. Or it could arrive in six years, according the Cloud Security Alliance's countdown. Preparing for that future, as the authors assert, benefits from government initiative. Post-quantum cybersecurity will necessitate government-wide standardization alongside industry adoption of the National Institute of Standards and Technology's (NIST) post-quantum algorithms. The Biden administration should be credited for ushering the country toward achieving post-quantum cryptographic agility. Transitioning to post-quantum cybersecurity, as with energy, demands that government offer remedies that ensure the private sector is acting to protect users.

Widespread electrification, similarly, requires cybersecurity standardization for the coming tide of new energy storage, generation, and transmission. Biden's cyber team recognizes that foregrounding cyber resilience into energy infrastructure at the dawn of an energy transformation is a weighty task. National Labs and the Department of Energy will spearhead the effort to prevent states and the private sector from implementing a "patchwork of security controls" without necessary cybersecurity for devices and sensors. The technical solution, however, hinges on government preserving its funding of research and development to steer the market toward creating secure opportunities for users.

Pillar four zooms in to fix "innovation without security" with the smart application of federal power, including spending. Government's reassertion of its agency in shaping the innovation ecosystem has been a priority of the Biden administration. Two laws—the Inflation Reduction Act and the CHIPS and Science

Act—exemplify how the Biden administration views the urgency of government returning to its Cold War-era championing of innovation. The Cyber Strategy spells out funding priorities and documents how a bevy of government institutions are poised to implement a new cyber social contract: the National Science Foundation, NIST, the Department of Energy and its complex of National Labs, and Federally Funded Research and Development Centers. By harmonizing ways, means, and ends, Inglis's team advocates for a cyber social contract that promotes innovation.

The genesis of the strategy's new cyber social contract was detailed in Inglis's and Harry Krejsa's *Foreign Affairs*article "The Cyber Social Contract: How to Rebuild Trust in a Digital World." The authors noted that misaligned incentives against a backdrop of cyber volatility left the nation, the private sector, and citizens at persistent risk. National security and citizens' daily lives were imperiled without a reset, they wrote. Impending waves of digitization would embolden malicious actors to prey upon the staggering number of vulnerabilities. "With a shared and affirmative vision, the public and private sectors can build a new social contract," the authors insisted, "without undermining the integrity and vitality essential to an innovative economy."

How does the blueprint in the *Foreign Affairs* article differ from the administration's cybersecurity strategy document? Inglis and Krejsa avoid a discussion of responsible regulation, as public interest technologist Bruce Schneier commented. Schneier lauded the article but tempered his praise by asserting that "regulation is how society aligns market incentives with its own values." Without explicitly foregrounding the state's power to wield a regulatory hammer, Inglis and Krejsa cannot fully embrace the fundamental element of state authority in crafting a new social contract for cybersecurity. The National Cyber Strategy, on the other hand, lays the foundation for modernizing how users, the private sector, and the state interact in the domain.

The strategy includes other notable changes, including the absence of any mention of deterrence and escalation that signals a victory for the adherents of Defend Forward—a strategy that intends to "disrupt or halt malicious cyber activity at its source." For years, General Paul Nakasone the dual-hatted Director of the National Security Agency and Commander of U.S. Cyber Command led a campaign to dislodge traditional deterrence theory from cyber strategy. Richard Harknett and Michael *Fischerkeller*'s 2017 "Deterrence is Not A Credible Strategy for Cyberspace" argued against voices who applied deterrence thinking to the nation's cybersecurity. Debates over deterrence persisted. The Cyberspace Solarium Commission formulated a strategy of layered cyber deterrence that welded Defend Forward onto its framework to restore deterrence. Ultimately, as evidenced in the cyber strategy document, deterrence is inadequate to tackle the gravity of technological threats that malicious actors will capitalize on.

The document serves as a testament to the foresight of the U.S. Cyberspace Solarium Commission's recommendation to stand up the National Cyber Director's office. Inglis's former office possesses the centralizing force to harmonize disparate interagency interests. The National Cyber Director recruits staff from across the government, private sector, and academia to obtain a 360-degree view of the threat landscape. Future administrations will likely turn to the National Cyber Director to publish cyber strategies that maintain the technical acumen and policy smarts in the 2023 report. The accomplishment, however, is less about the bureaucratic capabilities than the Cyber Strategy's ability to imagine a new operating dynamic for the nation's cybersecurity. Former Director Inglis and his staff are to be applauded for this sophisticated document.

Obstacles are present, most prominently one that involves how the private sector may resist regulation that could impede commercialization of new technologies. The reigning incentive structure rewards quick commercialization where security ranks below rushing products to market. Realigning priorities will require consistency across the Biden administration and subsequent presidencies that build upon experiences forged over the past year.

Pathways for collaboration improved as a result of the close public-private cooperation after the Russia-Ukraine War's onset in 2022. Anne Neuberger, the Deputy National Security Adviser for Cyber and

Emerging Technology, described it as “a coming-of-age for our cyber community.” Forging a new social contract for cyberspace after ransomware attacks like the 2021 Colonial Pipeline incident, high profile hacks, and the shift to cyber intrusion data sharing intersects with new threat awareness after the start of Russia’s invasion of Ukraine.

In this milieu, the Biden administration is employing the power of government to renegotiate the rules of cybersecurity. The National Cyber Strategy articulates a bold vision for renovating the cyber social contract, and action is necessary if not overdue. Attack surfaces that malicious actors and nations such as China and Russia will target are increasing at a staggering rate. Untenable risks require government intervention to align incentives and guarantee users are not prey due to the private sector’s errors. This administration and subsequent ones will face consistent cyber volatility. Action soon will ward off the market failures that endanger the nation’s digital ecosystem that is the woven into the fabric of Americans’ daily lives. A new cyber social contract is overdue, and it prepares the nation for the inescapable threats ahead.

