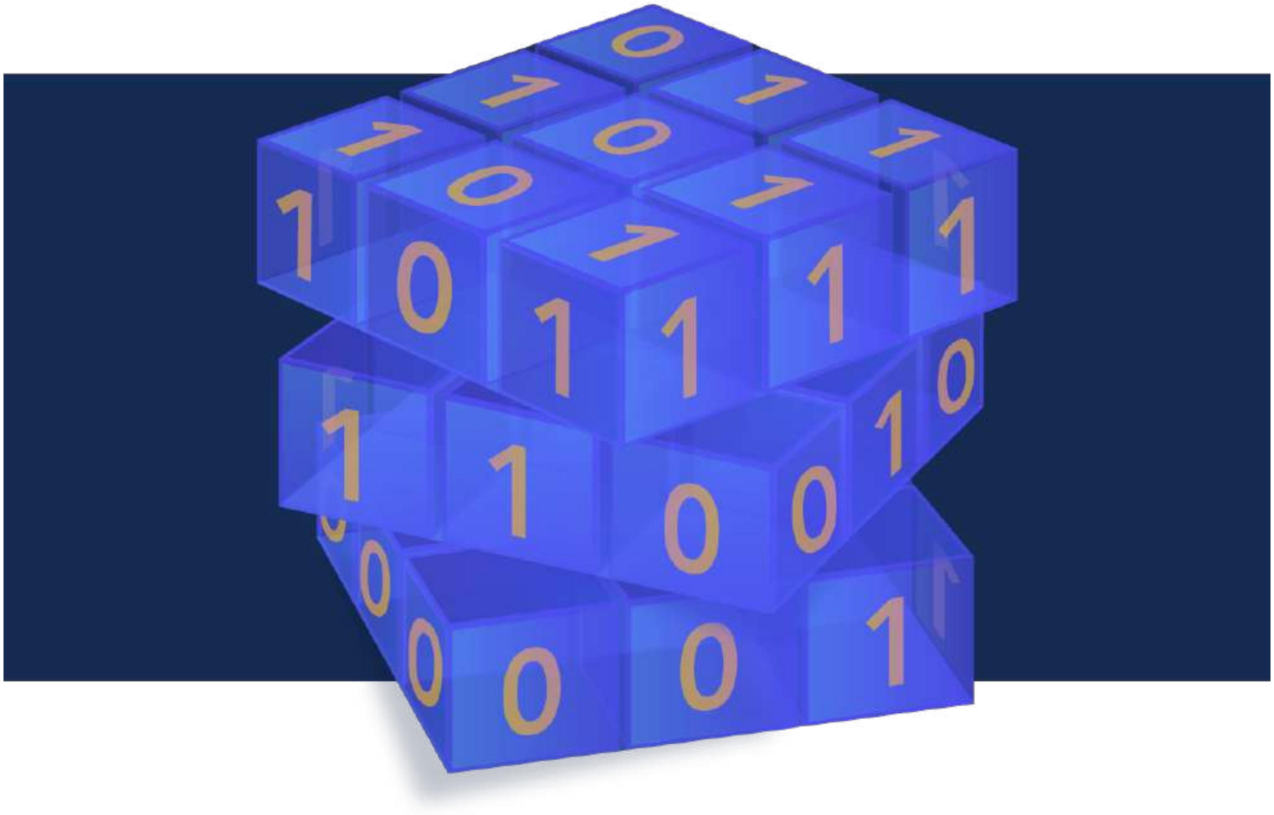
# Crypto News

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

## March 01, 2023



# TABLES OF CONTENTS

# Editorial

Happy March Readers! What are your plans for Spring Break? Whatever they may be, make sure to make some time for this month's issue of CryptoNews!

Let's start with an interesting new study which claims that cybersecurity may also benefit from digital twins. For those who work with digital twins, you know that digital twins are virtual copies of physical items. Industries including healthcare, aerospace, and automotives are using digital twins to help with decision making based on analysis and modeling of real-time data from the physical items. Now, imagine using the abundance of information gathered by a digital twin in order to detect cyber-attacks. Skeptical? The authors of the study claim that it can be done. Scroll down to article 5 to read more about the claims and judge for yourself.

We've had articles in the past highlight how quantum computers can help the automotive industry. This time let's pivot to an article highlighting the dangers quantum computers pose. Article 25 takes the time to dive into the nuances of quantum computing as well as the automotive industry and how the latter will be impacted by the former. What I truly appreciate about the article is the simple but terrifying use case presented in the section titled "Fast forward to 2035: Future attack scenario" which can be used to convince decision makers of the threats involved. I agree with the author that presenting use cases is an effective form of conveying information about a potential threat and though I'm always a proponent of using real-life examples once available, in the case of quantum computers, it will be far too late to make changes if we wait that long. The potential for the level of destruction and loss of life must be avoided, not considered inevitable and allowed to happen before changes are made. Long story short, start preparing now!

We do hope you'll find this month's issue as enlightening and interesting as we did. As always, happy reading!

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

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

# 1.ID Quantique, KCS And SK Telecom Release A New Quantum Enhanced Cryptographic Chip At MWC23

by MENAFN
https://menafn.com/1105669289/ID-Quantique-KCS-And-SK-Telecom-Release-A-New-Quantum-Enhanced-Cryptographic-Chip-At-MWC23

Ultimate security for connected devices and IoT systems: combining IDQ's QRNG and KCS' cryptographic communication semiconductor into one security chipset.

**Even the simplest and least expensive IoT device needs to have the highest level of security as people health and safety can be compromised.**" - Grégoire Ribordy, CEO and co-founder of ID QuantiqueBARCELONA, SPAIN, February 28, 2023 /einpresswire.com / -- Ultimate security for connected devices and IoT systems: combining IDQ's quantum random number generator (QRNG) technology and KCS' cryptographic communication semiconductor technology into one security chipset. This next generation security chip provides the highest level of security for IoT and connected devices and unrivalled protection against hacking.

In a digital and interconnected world, people and companies are using IoT connected devices for more and more services and applications, from healthcare to personal finance and the monitoring of industrial and utility processes. As with almost all connected and communication technologies, there comes an associated cybersecurity risk raising the need for security to the edge.

Today, at Mobile World Congress in Barcelona, SK Telecom and ID Quantique, the world leader in Quantum-Safe security solutions, present this new quantum-enhanced cryptographic chip co-developed with Korea Computer & Systems (KCS), a maker of IoT security cryptographic chips to secure IoT devices communication.

This quantum-enhanced cryptographic chip is an ultra-compact and low-power chip that provides strong security functions to various IoT-based products and devices. Adding ID Quantique's ultra-compact qrng chip (IDQ250C3) to KCS' crypto chip ensures trusted authentication and encryption of sensitive information and make our connected world more secure. The combination of these two chips into one chipset is more cost effective and a compact solution, allowing board size to be reduced by 20% thanks to a higher integration level, compared to the case of mounting two existing and separate chips on a board. In addition, the new chip is in the process of acquiring the highest level of security from the Korean National Intelligence Service's KCMVP certification body. It targets the fast-growing security market with applications from national defense sectors to industrial and public sectors.

KCS, SK Telecom and IDQ have been collaborating for several years, bringing to the market a whole range of crypto chip-based solutions aiming at ensuring and enhancing IT security without compromising on performance and speed.

The effectiveness of any cryptographic system is associated with the encryption keys it uses. In turn, the strength of the key directly depends on the degree of randomness used in its generation. ID Quantique was the first company to develop a quantum random number generator (QRNG) in 2001 and it has remained the market leader in terms of reliability and certifications, with its quantis qrng product family . ID

Quantique's chips can easily be embedded in a wide variety of hardware security modules, data encryptors, IoT devices, communications systems for autonomous vehicles, drones, satellites, etc. QRNGs generate provably unbiased and totally unpredictable randomness with the highest entropy from a CMOS image sensor, using ID Quantique patented quantum technology.

At ID Quantique, we also focus on providing long-term security solutions for our customers' IT infrastructures. Our quantum key distribution (qkd) solution is used to upgrade existing fiber optic telecommunication infrastructures by providing provably secure and unhackable key exchange for data encryption and to guarantee data security and confidentiality for the long-term. Our 4th generation QKD System will be displayed at MWC (booth in Hall 3 Stand 3I30).

'We unveil for the first time at MWC23 a 'quantum enhanced crypto chip' that provides strong security functions while increasing economic efficiency." Ha Min-yong, CDO of SK Telecom

"KCS has a long-established reputation in the security field. For over forty years we have been developing and integrating security-first solutions and software. With the addition of IDQ's ultra-small chip, we will be able to guarantee the highest level of security on the market." Kwang-mook Kim, CEO of KCS

"Even the simplest and least expensive IoT device needs to have the highest level of security as people health and safety can be compromised. The combination of our 2 chips in 1 quantum-enhanced crypto chip guarantees the highest level of trust for consumers." Grégoire Ribordy, CEO and co-founder of ID Quantique

# 2.Google Achieves Quantum Error Correction Milestone: Sundar Pichai

by Sundar Pichai
https://blog.google/inside-google/message-ceo/our-progress-toward-quantum-error-correction/

Three years ago, our quantum computers were the first to demonstrate a computational task in which they outperformed the fastest supercomputers. It was a significant milestone on our roadmap toward building a large-scale quantum computer, and the "hello world" moment so many of us had been hoping for. Yet in the long arc of scientific progress it was just one step towards making quantum applications meaningful to *human* progress.

Now, we're taking another big step forward: For the first time ever, our Quantum AI researchers have experimentally demonstrated that it's possible to reduce errors by increasing the number of qubits. In quantum computing, a qubit is a basic unit of quantum information that can take on richer states that extend beyond just 0 and 1. Our breakthrough represents a significant shift in how we operate quantum computers. Instead of working on the physical qubits on our quantum processor one by one, we are treating a group of them as one logical qubit. As a result, a logical qubit that we made from 49 physical qubits was able to outperform one we made from 17 qubits. *Nature* is publishing our research today.

Here's why this milestone is important: Our quantum computers work by manipulating qubits in an orchestrated fashion that we call quantum algorithms. The challenge is that qubits are so sensitive that even stray light can cause calculation errors — and the problem worsens as quantum computers grow. This has significant consequences, since the best quantum algorithms that we know for running useful applications require the error rates of our qubits to be far lower than we have today. To bridge this gap, we will need quantum error correction.

Quantum error correction protects information by encoding it across multiple physical qubits to form a "logical qubit," and is believed to be the only way to produce a large-scale quantum computer with error rates low enough for useful calculations. Instead of computing on the individual qubits themselves, we will then compute on logical qubits. By encoding larger numbers of physical qubits on our quantum processor into one logical qubit, we hope to reduce the error rates to enable useful quantum algorithms.

It's the first time anyone has achieved this experimental milestone of scaling a logical qubit. We've been working towards this milestone and the ones ahead because quantum computers have the potential to bring tangible benefits to the lives of millions. Someday, we believe quantum computers will be used to identify molecules for new medicines, create fertilizer using less energy, design more efficient sustainable technologies from batteries to nuclear fusion reactors, and produce physics research that will lead to advances we can't yet imagine. That's why we're working on eventually making quantum hardware, tools and applications available to customers and partners, including through Google Cloud, so that they can harness the power of quantum in new and exciting ways.

Helping others to realize the full potential of quantum will require us to achieve even more technical milestones in order to scale to thousands of logical qubits with low error rates. There's a long road ahead — several components of our technology will need to be improved, from cryogenics to control electronics to the design and materials of our qubits. With such developments, large-scale quantum computers will come into clearer view. Developing quantum processors is also an excellent testbed for AI-assisted engineering as we explore the use of machine learning to improve our processes.

We are also taking steps to develop quantum computing responsibly, given its powerful potential. Our partnerships with governments and the security community are helping to create systems that can protect internet traffic from future quantum computer attacks. And we're making sure services like Google Cloud, Android and Chrome remain safe and secure in a quantum future.

I am inspired by what quantum computing could mean for the future of our users, customers and partners, and the world. We'll continue to work towards a day when quantum computers can work in tandem with classical computers to expand the boundaries of human knowledge and help us find solutions to some of the world's most complex problems.

# 3.Comments On Google's Quantum Error Correction Announcement

**by GQI**
https://quantumcomputingreport.com/comments-on-googles-quantum-error-correction-announcement/

Earlier this week, the Google AI Quantum team announced it has made additional progress on quantum error correction and had just published a paper in *Nature* magazine with the technical details. In brief, to solve the problem of relatively high error rates in a single quantum physical qubit, engineers can group together several of the physical qubits together to create a single logical qubit which, if done properly, will show a decreased error rate from the physical qubit.

What Google demonstrated was that the logical error rate of a logical qubit composed of 49 physical qubits (code distance 5) was lower than the error rate of a logical qubit composed of 17 physical qubits (code distance 3). While it may appear obvious that when you scale up the number of physical qubits the error rate will decrease, in practice it is not so easy because the more physical qubits you add, the higher the probability that some of those physical qubits will incur errors and the larger code won't show an improvement in the error rate. What the Google AI team demonstrated for the first time is that with careful engineering it is indeed possible to scale the error correction codes. In their experiment, they reduce the logical error rate from 3.028% for a 17 physical qubit implementation to 2.914% for a 49 physical qubit implementation. Although the improvement is extremely small and nowhere near what would be needed for a practical error corrected quantum computer, it is at least, going in the right direction.

Although a lot of hoopla was generated in the popular press about this, regular readers of the *Quantum Computing Report* may remember that we first reported on this research in our July 2022 Research Roundup report when this was first posted on arXiv as a pre-print paper. It's still an impressive accomplishment, but should still be regarded as one of many milestones that the industry will need to achieve in order to have a fully corrected fault tolerant quantum computer. This one accomplishment won't change the industry overnight and it will still take many years to reach the final goal.

We should note that error correction is one of the most active areas of research within quantum computing and many groups have also achieved significant results. (However, those other teams may not have spent as much money as the Google PR team did in promoting the accomplishments!) Notable papers we have seen in the past few years include one from IonQ, University of Maryland, and Duke University titled *Fault-Tolerant Operation of a Quantum Error-Correction Code* which encoded a logical qubit from 13 physical qubits to show an improvement. Another one came from Quantinuum titled *Implementing Fault-tolerant Entangling Gates on the Five-qubit Code and the Color Code* which demonstrated entangling gates between two logical qubits done in a fully fault-tolerant manner using real-time error correction. And also a previous Google paper titled *Exponential suppression of bit or phase errors with cyclic error correction* which demonstrated an improvement in reducing either bit-flip error or phase-flip errors, but not both at the same time.

We expect to see many more similar papers from multiple parties over the next few years with each making one more step forward. To put the magnitude of the problem in perspective, some of the really significant quantum applications that we always talk about will require programs that contain hundreds of thousands of logical gates with each gate having a logical qubit error rate of perhaps $10^{-15}$. Today, we are roughly at the $10^{-3}$ level so an improvement of over 10 orders of magnitude is still required. So a lot of research and hard work will be required in pretty much all areas of the system including architecture, algorithms, material science, fabrication, control electronics, mechanicals, and integration with the classical processor.

# 4.Quantinuum Sets Industry Record For Hardware Performance With New Quantum Volume Milestone

by Matt Swayne
https://thequantuminsider.com/2023/02/23/quantinuum-sets-industry-record-for-hardware-performance-with-new-quantum-volume-milestone/

Quantinuum, the world's largest standalone integrated quantum computing company, today announced its H1 generation quantum processors set two performance records in quick succession, with its H1-1 achieving a quantum volume (QV) of 16,384 (2^14), and then 32,768 (2^15). The achievements represent a high-water mark for the quantum computing industry, based on the widely recognized QV benchmark, which was originally developed by IBM to reflect a quantum computer's general capability.

"Quantum volume is crucial to the ongoing development and research necessary to create the bigger and better quantum computers needed to achieve a quantum advantage," said Paul Smith-Goodson, Analyst, Moor Insights and Strategy. "Quantinuum has prioritized increasing its quantum volume since the start, which has not only benefitted its current applications but set itself up to be the benchmark in achieving quantum advantage."

This marks the eighth time in less than three years that Quantinuum's H-Series, which is based on quantum charge coupled device technology, has set an industry benchmark, and fulfills a public commitment made in March 2020 to increase the performance of the H-Series quantum processors, Powered by Honeywell, by an order of magnitude each year for five years.

"This is a remarkable milestone for quantum computing and inline with the technology we have seen from Quantinuum," said Marco Pistoia, Ph.D., Distinguished Engineer and Head of Global Technology Applied Research, JPMorgan Chase. "As evidenced in our research, we have produced groundbreaking algorithms on their quantum computers for the past several years, which has allowed us at JPMorgan Chase to be on the leading edge of quantum computing. We look forward to continuing to make more breakthroughs in quantum computing together."

To provide more detail on the underlying technological improvements that led to the new benchmark, Quantinuum revealed details of recent performance enhancements to the H-Series, including reductions in the phase noise of the device's lasers, reducing two-qubit gate error and memory error, and improvements to elements of the calibration process. Scientists at Quantinuum also shared insights into how the improvements that resulted in the new benchmark reduce the time it takes for algorithms to run, improve the ability to run quantum error correction codes, and lead to better results for the scientists and researchers using the H-Series hardware.

"We are exactly where we expect to be on our roadmap," said Tony Uttley, President and COO of Quantinuum. "Our hardware team continues to deliver technical improvements right across the board, and our approach of continuously upgrading our quantum computers means that these are felt immediately by our customers."

A five-digit QV number is very positive for real-time quantum error correction (QEC) because of the low error rates, number of qubits, and very long circuits. QEC is a critical ingredient to large-scale quantum computing and the sooner it can be explored on today's hardware, the faster it can be demonstrated at large-scale.

"With the technology improving fast, we do everything we can to help our customers and the community understand how we are achieving such rapid progress," said Jenni Strabley, Senior Director of Offering Management at Quantinuum. "Which is why we have published the data behind the results we announced today. Our goal is to accelerate quantum computing, and that is something we can only achieve as an industry."

Further details on the Quantum Volume tests: https://quantum-journal.org/papers/q-2022-05-09-707/

Quantinuum's GitHub repository for Quantum Volume data: https://github.com/CQCL/quantinuum-hardware-quantum-volume

Quantinuum's GitHub repository for hardware specifications: https://github.com/CQCL/quantinuum-hardware-specifications

# 5.How Digital Twins Could Protect Manufacturers From Cyberattacks

by Jonathan Griffin
https://www.nist.gov/news-events/news/2023/02/how-digital-twins-could-protect-manufacturers-cyberattacks

Detailed virtual copies of physical objects, called digital twins, are opening doors for better products across automotive, health care, aerospace and other industries. According to a new study, cybersecurity may also fit neatly into the digital twin portfolio.

As more robots and other manufacturing equipment become remotely accessible, new entry points for malicious cyberattacks are created. To keep pace with the growing cyber threat, a team of researchers at the National Institute of Standards and Technology (NIST) and the University of Michigan devised a cybersecurity framework that brings digital twin technology together with machine learning and human expertise to flag indicators of cyberattacks.

In a paper published in *IEEE Transactions on Automation Science and Engineering*, the NIST and University of Michigan researchers demonstrated the feasibility of their strategy by detecting cyberattacks aimed at a 3D printer in their lab. They also note that the framework could be applied to a broad range of manufacturing technologies. Cyberattacks can be incredibly subtle and thus difficult to detect or differentiate from other, sometimes more routine, system anomalies. Operational data describing what is occurring within machines — sensor data, error signals, digital commands being issued or executed, for instance — could support cyberattack detection. However, directly accessing this kind of data in near real time from operational technology (OT) devices, such as a 3D printer, could put the performance and safety of the process on the factory floor at risk.

“Typically, I have observed that manufacturing cybersecurity strategies rely on copies of network traffic that do not always help us see what is occurring inside a piece of machinery or process,” said NIST mechanical engineer Michael Pease, a co-author of the study. “As a result, some OT cybersecurity strategies seem analogous to observing the operations from the outside through a window; however, adversaries might have found a way onto the floor.”

Without looking under the hood of the hardware, cybersecurity professionals may be leaving room for malicious actors to operate undetected.

## Taking a Look in the Digital Mirror

Digital twins aren’t your run-of-the-mill computer models. They are closely tied to their physical counterparts, from which they extract data and run alongside in near real time. So, when it’s not possible to inspect a physical machine while it’s in operation, its digital twin is the next best thing.

In recent years, digital twins of manufacturing machinery have armed engineers with an abundance of operational data, helping them accomplish a variety of feats (without impacting performance or safety), including predicting when parts will start to break down and require maintenance.

In addition to spotting routine indicators of wear and tear, digital twins could help find something more within manufacturing data, the authors of the study say.

“Because manufacturing processes produce such rich data sets — temperature, voltage, current — and they are so repetitive, there are opportunities to detect anomalies that stick out, including cyberattacks,” said Dawn Tilbury, a professor of mechanical engineering at the University of Michigan and study co-author.

To seize the opportunity presented by digital twins for tighter cybersecurity, the researchers developed a framework entailing a new strategy, which they tested out on an off-the-shelf 3D printer.

The team built a digital twin to emulate the 3D printing process and provided it with information from the real printer. As the printer built a part (a plastic hourglass in this case), computer programs monitored and analyzed continuous data streams including both measured temperatures from the physical printing head and the simulated temperatures being computed in real time by the digital twin.

The researchers launched waves of disturbances at the printer. Some were innocent anomalies, such as an external fan causing the printer to cool, but others, some of which caused the printer to incorrectly report its temperature readings, represented something more nefarious.

So, even with the wealth of information at hand, how did the team’s computer programs distinguish a cyberattack from something more routine? The framework’s answer is to use a process of elimination.

The programs analyzing both the real and digital printers were pattern-recognizing machine learning models trained on normal operating data, which is included in the paper, in bulk. In other words, the models were adept at recognizing what the printer looked like under normal conditions, also meaning they could tell when things were out of the ordinary.

If these models detected an irregularity, they passed the baton off to other computer models that checked whether the strange signals were consistent with anything in a library of known issues, such as the printer’s fan cooling its printing head more than expected. Then the system categorized the irregularity as an expected anomaly or a potential cyber threat.

In the last step, a human expert is meant to interpret the system’s finding and then make a decision. “The framework provides tools to systematically formalize the subject matter expert’s knowledge on anomaly detection. If the framework hasn’t seen a certain anomaly before, a subject matter expert can analyze the collected data to provide further insights to be integrated into and improve the system,” said lead-author Efe Balta, a former mechanical engineering graduate student at the University of Michigan and now a postdoctoral researcher at ETH Zurich.

Generally speaking, the expert would either confirm the cybersecurity system’s suspicions or teach it a new anomaly to store in the database. And then as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

In the case of the 3D printer, the team checked its cybersecurity system’s work and found it was able to correctly sort the cyberattacks from normal anomalies by analyzing physical and emulated data. But despite the promising showing, the researchers plan to study how the framework responds to more varied and aggressive attacks in the future, ensuring the strategy is reliable and scalable. Their next steps will likely also include applying the strategy to a fleet of printers at once, to see if the expanded coverage either hurts or helps their detection capabilities.

“With further research, this framework could potentially be a huge win-win for both maintenance as well as monitoring for indications of compromised OT systems,” Pease said.

# 6.IBM, Vodafone, And GSMA Members Outline Critical Pathways To Protect Telcos Against Quantum-Era Cyberthreats

by Resham Parikh
https://newsroom.ibm.com/2023-02-23-IBM,-Vodafone,-Other-GSMA-Taskforce-Members-Outline-Critical-Pathways-to-Protect-Telcos-Against-Quantum-Era-Cyberthreats

As part of the Post-Quantum Telco Network Taskforce, GSMA has published, with contributions from members IBM, Vodafone, and others, the Post Quantum Telco Network Impact Assessment: an in-depth analysis of the quantum security threats facing the telecommunications industry and a detailed, step by step list of potential solutions to prepare for these threats.

The report, which debuted ahead of GSMA's annual Mobile World Congress in Barcelona, maps out a clear path for telco organizations to work across their ecosystems to protect data from cybercriminals acting today to tap into the potential power of future quantum computers. It includes:

- A telco-specific assessment of the business risk of quantum cyber threats, including four of the highest impact attack types: store now, decrypt later; code signing and digital signatures; rewriting history; and key management attacks.

- Discussion of standardization for hardware and software changes, such as SIM cards, public key infrastructure, digital certificates and CPE devices.

- Specific approaches to quantum-safe algorithms and risk assessment frameworks, including code-based, lattice-based, hash-based, multivariate-based, and hybrid approaches.

- Timelines of several government plans that have been launched to implement quantum-safe encryption (Australia, Canada, China, France, Germany, Japan, New Zealand, Singapore, South Korea, the UK and the U.S.).

- Examples of quantum-safe applications to several telco domains, including devices, 5G networks, SIMs, Operating systems, ERP, infrastructure and the cloud.

According to the report, it is widely considered that by 2032 there will be completion of a large fault-tolerant quantum computer capable of running crypto-analytic algorithms that could threaten current cryptographic approaches.

The advent of such technology requires immediate preparation, as some forms of attack may be retrospective (e.g. "store now, decrypt later"). Motivated bad actors may be harvesting and storing data now in order to decrypt it once certain quantum computing capabilities become available. As stated in the report, such actors may do this to "undermine the security of data with long-lived confidentiality needs, such as corporate IP, state secrets or individual bio-data."

To learn more about these issues and what can be done today to protect against future quantum attacks, download the Post Quantum Telco Network Impact Assessment.

IBM has spent years building a global team of cryptography experts to develop quantum-safe schemes and preparation plans. Just in the last year, IBM not only contributed to the development of three of the four algorithms chosen in 2022 by the US National Institute of Standards and Technology (NIST) for post-quantum cryptography standardization; the team also deployed the industry's first quantum-safe system, IBM z16; launched a suite of IBM Quantum Safe services; and was an initial member of the GSMA Post-Quantum Telco Network Taskforce.

# 7.How Can Quantum Entanglement Be Used For Secure Communication?

by James Dargan
https://thequantuminsider.com/2023/02/20/quantum-entanglement-communication/

## Faster Than Light?

Known as FTL, faster-than-light travel and communication is the theory that matter (or information) can travel faster than the speed of light. According to Einstein's special theory of relativity, however, nothing in nature can travel faster than the speed of light except for photons, which possess zero rest mass.

Nevertheless, the hypothetical particle called the tachyon — named by particle physicist Gerald Feinberg in his 1967 paper titled *"Possibility of faster-than-light particles"* — has been theorized to exceed the speed of light. Yet, its mere existence as a phenomenon would contravene causality and mean that time travel was indeed possible, a claim the general scientific community professes as unfeasible as a hypothesis.

With the basic theory described as to the faster-than-light conundrum, this, then, brings us to the topic at hand: what is quantum entanglement communication and how is the faster-than-light travel theory connected to quantum communication?

## What Exactly is Quantum Entanglement Communication?

To really understand quantum entanglement-based communication, one should first understand what quantum entanglement is. First put out there by Einstein, Podolsky and Rosen as "spooky action at a distance", which has its roots in the argument about quantum entanglement and quantum superposition first developed in the 1920s and 1930s, entanglement infers the phenomenon that communication occurs instantly. Put simply, it is when two particles are bound together no matter the physical distance between them.

Even so, though quantum particles that are entangled appear to interact with each other instantaneously — no matter the distance and thus moving at the speed of light — modern science's understanding of quantum mechanics interprets that it is impossible to transmit data using quantum entanglement. And it is here that a stumbling block lies in a robust and workable model of quantum entanglement communication. To be able to transmit or communicate information, you must send data, and this is impossible using quantum entanglement. If it's true, though, and quantum entanglement communication becomes possible one day, its applications could have far-reaching effects on things like sensing technology and secure information transfer.

The French physicist Serge Haroche, one of the winners of the 2012 Nobel Prize in physics for trapping and manipulating individual particles while preserving their quantum nature, was interviewed in October

2022 in El Pais. When asked the question what Alain Aspect, John F. Clauser and Anton Zeilinger's joint 2022 Nobel Prize win for "experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science, means for quantum communication, his answer was expectantly informative:

"[…] Basic features of entanglement have been explored for 40 years, trying to demonstrate what happens when photons remain connected by that immaterial link called entanglement even when they're kilometers away. At that time there was no application for that experiment. It took 20 years until experiments like ours showed that it's possible to manipulate isolated quantum systems. Now, quantum communication has become very fashionable and has been improved. Now people will believe that it could be useful for something."

Making the case stronger, in January of this year, researchers in India demonstrated that photon entanglement in a *"certain continuous-variable basis revives itself as the photons propagate away from their source"*, which could be applicable for sending quantum information securely over long distances for some of the said applications above.

## What does Quantum Communication Mean for Cybersecurity?

There is little doubt that quantum technology will have a huge impact on cybersecurity and cryptography. Already, we can see government agencies across the globe preparing enterprises for "Q-Day", a time when quantum computers will be able to use Shor's algorithm to break all public key systems that use integer factorization-based cryptography.

As a procedure, quantum communication entails encoding information in quantum states, called qubits, rather than in the classical binary tradition of "zeros and ones", taking advantage of the special properties of these quantum states to guarantee security. Most commonly, photons are used for this.

Quantum Key Distribution (QKD) is a proven theoretical security that is future-proof yet requires trusted nodes for long distances. Presently, a single QKD link is limited to a few 100 km with a sweet spot in the 20–50 km range. Work on quantum repeaters and satellite-QKD is ongoing to extend the range. On the downside, full lifecycle costs are not yet known but there are increased hardware integration costs which could turn out to be prohibitive.

On the other hand, post-quantum cryptography (PQC) is another approach to future security issues that doesn't leverage quantum entanglement. Coming in lattice-based, code-based, hash-based, super-singular isogenies, and multivariate-quadratic, PQC security is still questionable. On the upside, however, this does come with long distance as the algorithms operate at the software layer.

Other constraints of this approach are that the software demands increased memory and/or time requirements and, similar to QKD, the costs of implementation are still unknown, though PQC algorithms do have the advantage here, as a chip-based approach to quantum security technologies costs are evidently falling and will continue to do so.

## Conclusion

As it stands, strides are being made in quantum technology and research which is boosting the possibility that one day in the future quantum entanglement-based communication will become a reality, aiding communication and cybersecurity and bringing us to a totally new technological epoch, as the continued research by physicists in quantum entanglement—the best example so far the 2022 Nobel Prize-winning trio of Aspect, Clauser and Zeilinger—is helping us move in that direction.

# 8.Quantum Computers And The Future Of Computing

by Adil Husnain
https://www.scoopearth.com/quantum-computers-and-the-future-of-computing/

The Future of Quantum Computing is a hot topic in the tech world today. Quantum computers are compelling and have the potential to revolutionize computing, with applications ranging from artificial intelligence to cryptography. With their promise of superior processing power, quantum computers could revolutionize the way we use technology, making computing faster and more efficient than ever. In this blog post, we'll explore what quantum computers are, how they work, and the possibilities they present for the Future of Computing.

## What is quantum computing?

Quantum computing is an emerging technology that uses the principles of quantum mechanics to process and store data. This type of computing is capable of performing calculations that are significantly faster than traditional computers. Quantum computers are real, and many leading companies invest in developing quantum computing hardware and software.

Quantum computers can solve complex problems such as optimization, cryptography, and artificial intelligence more efficiently than traditional computers. Quantum computing has been around for some time, but only recently has it become feasible due to advances in hardware and software technologies.

Quantum computing companies like IBM, Google, Microsoft, and Intel have been actively developing this technology, with each company focusing on different areas of quantum computing.

Quantum computers use the principles of quantum mechanics to store and process information. It uses qubits (quantum bits), tiny particles representing 0s and 1s. The advantage of this is that a qubit can process multiple inputs at once, allowing for greater computing power.

## Benefits of quantum computing

Potential benefits of quantum computing:

- **Improved cryptography:**

  Quantum computing can break some encryption algorithms currently used to secure communication, such as the RSA algorithm. However, it can also enable new forms of cryptography that are more secure against quantum attacks.

- **Faster computation:**

  Quantum computers can solve specific problems much faster than classical computers, including optimization problems, simulation of quantum systems, and factorization of large numbers.

- **Enhanced artificial intelligence:**

Quantum computing can accelerate the development of machine learning algorithms and other AI applications by providing faster computation and the ability to process vast amounts of data.

- **Better weather forecasting:**

  Quantum computing can improve the accuracy of weather forecasting models by processing vast amounts of data and simulating complex interactions between the atmosphere and oceans.

- **Faster database searching:**

  Quantum computing can speed up the search of unsorted databases and could be used for tasks such as identifying patterns in large data sets.

- **More efficient logistics:**

  Quantum computing can optimize complex logistical problems, such as route optimization and supply chain management, resulting in more efficient and cost-effective transportation and distribution.

## Challenges of quantum computing

The idea of quantum computing is still relatively new, and many of its challenges are yet to be fully understood or addressed. We are still determining whether quantum computing will be successful. Questions like “Are quantum computers real?” have arisen as a result and “Will quantum computing be available to everyone?” remain unanswered. Additionally, there are concerns about the security of quantum computing. To make quantum computing viable, it must be highly secure and immune to malicious attacks.

Despite these challenges, companies such as Quantum Computing Inc are investing heavily in developing quantum computing technology and trying to overcome the barriers that stand in its way. Quantum computing will become a reality and be available to everyone. However, before that can happen, further research is needed to ensure that quantum computers are secure and reliable.

## What industries will be affected by quantum computing?

The future of quantum computing will significantly impact a range of industries. Already, research is being done to explore the potential applications of quantum computers in fields such as chemistry, materials science, healthcare, finance, and even artificial intelligence (AI). Quantum computing is a rapidly evolving field that has the potential to impact a wide range of industries.

Here are some of the industries that are likely to be affected by quantum computing:

- **Healthcare:** Quantum computing has the potential to revolutionize the field of healthcare by providing faster and more accurate analysis of large amounts of medical data. A new treatment or diagnostic tool may be developed due to this.

- **Finance:** Quantum computing can enable faster and more accurate financial modeling and analysis, leading to better investment decisions, fraud detection, and risk management.

- **Materials Science:** Quantum computing could help to accelerate the development of new materials by simulating the behavior of atoms and molecules, leading to the discovery of new materials with unique properties.

- **Energy:** Quantum computing could improve the efficiency of energy production and storage by optimizing complex systems and simulating the behavior of atoms and molecules in materials used in energy technologies.

- **Cyber security:** Quantum computing could pose a significant threat to current cryptographic systems, but it could also help to develop new and more secure encryption techniques that are resistant to attacks by quantum computers.

- **Transportation:** Quantum computing could help to optimize traffic flow and transportation networks, leading to more efficient and sustainable transportation systems.

- **Manufacturing:** Quantum computing could optimize manufacturing processes and improve the quality of manufactured products by simulating the behavior of atoms and molecules in materials used in manufacturing.

Overall, quantum computing has the potential to revolutionize a wide range of industries by enabling faster and more accurate analysis and optimization of complex systems.

## FAQs about Quantum Computers and the Future of Computing

- **What is the Future of Quantum Computing?**

  The future of quantum computing looks very promising. It promises to revolutionize the computing world and usher in an age of unprecedented capabilities and processing power. Quantum computers can solve complex problems much faster than classical computers and tackle tasks that were once considered impossible.

- **How will quantum computing change the world?**

  Quantum computing has the potential to revolutionize many industries, including healthcare, finance, transportation, energy, and more. By utilizing quantum computing's processing power, businesses can analyze massive datasets in minutes instead of hours or days. Additionally, quantum computing can be used to develop new materials, medicines, and technologies.

- **Is quantum computing secure?**

  Yes, quantum computing is incredibly secure due to its use of quantum entanglement. This form of encryption ensures that data is encoded using two entangled particles, making it virtually impossible to crack. Additionally, quantum cryptography makes it much harder for hackers to access sensitive data.

## Conclusions

The future of quantum computing is promising, and the potential implications are immense. Quantum computing could revolutionize many industries and create new opportunities for researchers and businesses. Though quantum computing is still in its infancy, advances in quantum technologies have already led to significant advancements in chemistry, cryptography, and machine learning. By continuing to explore the possibilities of this technology, we can unlock a future of unprecedented options for both business and science. The end of quantum computing looks bright, and its potential is truly limitless.

# 9.How Quantum Computing Threatens In-

# ternet Security

by Raúl Limón

https://english.elpais.com/science-tech/2023-02-18/how-quantum-computing-threatens-internet-security.html

Internet security – from the most common banking transaction to conversations on messaging platforms – rests mainly on cryptographic keys: strings of characters encrypted by an algorithm.

The difficulty to decipher these keys depends on factorization – the decomposition of an algebraic expression in the form of a product. That is to say: six is equal to three times two. But this simple operation becomes extraordinarily complex if the given number exceeds a relatively small number of digits.

Take a look at this number: 261980999226229. This algebraic expression has been factored by a crude quantum computer in an experiment by Chinese scientists. Published on *ArXiv* – an online archive run by Cornell University – this unreviewed study has exposed the vulnerability of the encryption system and, therefore, the vulnerability of our entire digital society.

“The fact that quantum computing is a risk for the encryption methods we use today is well known. In 1994, Peter Shor (a mathematician at MIT) showed that a quantum computer could solve the factorization problem efficiently,” warns Antonio Acín, a research professor at the Institute of Photonic Sciences (ICFO) in Barcelona, Spain.

This opinion is not unique. A 2020 paper put out by the UK’s National Cyber Security Centre acknowledges “the serious threat that quantum computers pose to long-term cryptographic security.”

The USA’s National Institute of Standards and Technology (NIST) has spent seven years looking for security algorithms that are resistant to quantum computing. However, some of the proposals have been cracked in just over two days with a laptop. Ward Beullens – of the IBM research center in Zurich, Switzerland – demonstrated this in 2022.

Most researchers think that, for the quantum threat to be feasible, further development of this fledgling science is still necessary. Shor’s algorithm – the formula to decipher current systems, called Rivest-Shamir-Adleman (or RSA) and based on large prime numbers – requires a robust quantum computer, without errors, and millions of qubits (basic units of information in a quantum computer). The last one unveiled – the IBM Osprey processor – has merely 433 qubits.

In the journal *Nature*, Guilu Long – a physicist at Tsinghua University in China – acknowledges that “increasing the number of qubits without reducing the error rate is not enough.”

“We think that [today’s] cryptography is safe because, at the moment, we don’t have an efficient factorization algorithm,” explains Acín. “Humanity has been trying to find it since classical Greece (...) but it could happen that tomorrow, some very clever mathematician finds this algorithm and knocks everything down. This clever mathematician could be a quantum computer. Today’s world of encryption may be vulnerable as soon as [this is developed].”

The ephemeral security that has allowed for the maintenance of digital society is now being questioned by a team led by Bao Yang, from Shanghai Jiaotong University, after they factored a 48-bit key with a computer of only 10 qubits. The Chinese group stated that, with 372 qubits, the developed factorization algorithm could break an RSA key of more than 600 digits.

However, Acín claims that the problem solved “isn’t impressive, as it can be done with classic computers.”

“They haven’t proven anything. They simply prove that, in this case, it has worked and, perhaps, in the future, it will continue to work.” According to the Spanish physicist, the expectation of being able to break an RSA key made up of 600 digits is excessive.

Scott Aaronson – an expert in quantum computing at the University of Texas – agrees. “This is one of the most actively misleading quantum computing articles I have seen in 25 years. And I’ve seen many,” he wrote on his blog, Shtetl-Optimized.

The work evades Shor’s algorithm and uses one by the mathematician Claus Schnorr – from Goethe University in Frankfurt, Germany – to factor integers.

“This is good because [the researchers] indicate that we should not stick to Shor’s algorithm – which we know requires a very powerful computer – and that the terms can be shortened if we look for an alternative. That’s interesting and original,” says Acín, acknowledging a merit of the Yang team’s publication.

In any case, the Chinese article has managed to highlight the vulnerability of the current encryption system – something that is of concern to companies and governments all over the world. On this subject, the Spanish physicist explains that he is working on two possible solutions. The first is to “replace factorization with other problems that are more difficult for a quantum computer.” It’s the formula that NIST has been looking for for seven years.

The second is to develop “schemes whose security is based on the laws of quantum physics.” This solution depends on the development of quantum computing itself – which is still in its infancy – and requires specific equipment.

Both ways forward are challenging, as the UK National Cyber Security Centre notes: “The transition to any form of new cryptographic infrastructure is a complex and costly process that needs to be carefully planned and managed. There are security risks as systems change and business continuity risks if there is an unforeseen dependency on cryptographic components.”

A team from the University of Tokyo led by Hiroyuki Tanaka has proposed in *iScience* an alternative security system called Cosmocat. It is based on muons – short-lived subatomic particles (2.2 microseconds) – that are only found in cosmic rays and in laboratories.

“Basically, the problem with our current security paradigm is that it relies on encrypted information and decryption keys that are sent over a network from sender to receiver. Regardless of the way the messages are encrypted, in theory, someone can intercept and use the keys to decrypt apparently secure messages. Quantum computers simply make this process faster,” Tanaka explains.

“If we dispense with this key-sharing idea and instead find a way to use unpredictable random numbers to encrypt information, the system might be immune. [Muons] are capable of generating truly unpredictable numbers.”

The proposed system is based on the fact that the speed of arrival of these subatomic particles is always random. This would be the key to encrypt and decrypt the message, if there is a synchronized sender and receiver. In this way, the sending of keys would be avoided, according to the Japanese team. However, muon detection devices are large, complex and power-hungry, limitations that Tanaka believes the technology could ultimately overcome.

# 10.6 Quantum Algorithms That Will Change Computing Forever

by Ayush Jain
https://analyticsindiamag.com/6-quantum-algorithms-that-will-change-computing-forever/

The impact of quantum computing spans across a range of industries, including finance, logistics, and cryptography.

We are on the cusp of a new era in computing, where the fundamental units of information processing are no longer classical bits but quantum bits, or *qubits*. This shift is opening up a vast, new landscape of possibilities for tackling complex mathematical problems that classical computers can't solve efficiently.

To give a case in point, Google quantum computers are said to be 158 million times faster than the most sophisticated supercomputer existing today—which means that the task which the Boolean logic computers will take ten years to complete, these computers will be able to do in three seconds.

In the near future, the impact of quantum computing—spanning across a range of industries, such as finance, logistics, and cryptography—will be apparent to all.

Here is a list of some of the most popular quantum algorithms highlighting the significant impact quantum can have on the classical world:

## Shor's Algorithm

Our entire data security systems are based on the assumption that factoring integers with a thousand or more digits is practically impossible. That was until Peter Shor in 1995 proposed that quantum mechanics allows factorisation to be performed in polynomial time, rather than exponential time achieved using classical algorithms.

The runtime of classical factoring algorithms, such as the general number field sieve (GNFS), grows exponentially with the number of digits in the integer to be factored. Shor's algorithm, on the other hand, is a quantum algorithm for factoring integers that has polynomial runtime, meaning that the amount of time it takes to factor an integer grows only polynomially with the number of digits in the integer.

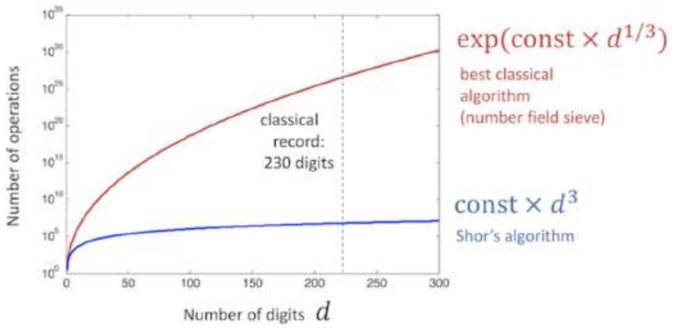


Figure 1: classical vs. quantum factoring algorithms

Here is one variant of Shor's algorithm by Alexey Kitaev, which reduces the number of qubits required to perform the factorisation, but nevertheless is able to clock a runtime roughly around d^3. You can check out the Qiskit implementation here.

## Grover's Algorithm

Developed by an Indian-American computer scientist, Grover's Algorithm is widely recognised as one of the most important quantum algorithms after Shor's algorithm. Its primary use is to accelerate unstructured search problems quadratically, but it also serves as a valuable tool, or subroutine, to obtain quadratic run time improvements for a variety of other algorithms.

Imagine you have a list of N items and you're trying to find one unique item in the list. A classical computer would need to check on average N/2 items in the list to find the unique item and, in the worst-case scenario, it would have to check all N items.  However, with quantum computing, Grover's amplitude amplification can significantly reduce the number of steps to roughly √N, which is a quadratic speedup compared to classical algorithms.

You can check out the Qiskit implementation here.

## Deutsch–Jozsa Algorithm

The Deutsch-Jozsa algorithm is a quantum algorithm designed to solve the 'Deutsch-Jozsa problem'. This problem involves determining whether a given Boolean function is 'constant' (i.e., returns the same output for all possible inputs) or 'balanced' (i.e., returns different outputs for at least one input pair) with the least number of queries.
For *n* bits as inputs, the classical algorithm requires minimum two calls to maximum 2^(n-1)+1 to be certain if a given function is constant or balanced, while the quantum computer can solve this using only one call to the function *f(x)*.  You can check out the Qiskit implementation here.

## Bernstein–Vazirani Algorithm

Like the Deutsch–Jozsa problem, the Bernstein–Vazirani algorithm also solves a specific black box problem. The problem involves finding *s* in the function f(x) = s . x, where *s* is some unknown string and . denotes the bitwise product (i.e., AND) operation.

Given an input *x*, a classical algorithm would need to call the function *f(x)* multiple times and use the results to determine the bits of *s* one at a time, requiring *n* calls to the function to recover the full string. However, a quantum computer can solve the problem with 100% confidence after only one call to the function *f(x)*.You can check out the Qiskit implementation here.

## Simon's Algorithm

Simon's was the first algorithm that showed an exponential speed-up versus the best classical algorithm in solving a specific problem.

The problem at hand involves a function *f(x)* for there are only two outcomes—either it maps each unique input to a unique output (one-to-one) or maps two distinct inputs to one unique output (two-to-one). Additionally, there is an unknown string *s* which is such that for all input strings *x*, f(x) is equal to f(x⊕s).

If the value of *s* is non-zero, then the function *f* is two-to-one, whereas when *s* is the zero string, the function *f* is one-to-one. Therefore, the objective is to determine whether the function *f* is one-to-one or two-to-one by simply finding the secret string *s*.

Classically, the value of *s* can be found for a function *f* with certainty by checking up to 2^(n/2) function calls. But, with quantum, using exponentially fewer queries—only a little more than *n* calls—a solution with 100% certainty can be found. You can check out the Qiskit implementation here.

### Quantum phase estimation (QPE) algorithm

QPE is an important subroutine that serves as a central building block for many quantum algorithms. The algorithm basically estimates the phase of an eigenvalue of a unitary operator. In other words, given a unitary operator *U* and an eigenvector |ψ〉 such that U|ψ〉 = e^(2πiθ)|ψ〉, where θ is the unknown phase angle, the goal of QPE is to estimate θ.

It is used in a wide range of applications including quantum simulation, quantum chemistry, and optimisation. You can read more about it here.

## 11.2023 Could Be The Breakthrough Year For Quantum Computing

by Richard Murray
https://venturebeat.com/data-infrastructure/2023-could-be-the-breakthrough-year-for-quantum-computing/

2022 has been a dynamic year for quantum computing. With commercial breakthroughs such as the UK Ministry of Defence (MoD) investing in its first quantum computer, the launch of the world's first quantum computer capable of advantage over the cloud and the Nobel Prize in Physics awarded for groundbreaking experiments with entangled photons, the industry is making progress.

At the same time, 2022 saw the tremendous accomplishment of the exaflop barrier broken with the Frontier supercomputer. At a cost of roughly $600 million and requiring more than 20 megawatts of power, we are approaching the limits of what classical computing approaches can do on their own. Often for practical business reasons, many companies are not able to fully exploit the increasing amount of data available to them. This hampers digital transformation across areas most reliant on high-performance computing (HPC): healthcare, defense, energy and finance.

To stay ahead of the curve, 91% of global business leaders are investing or planning to invest in quantum computing. According to reports, 70% are developing real-life use cases and 61% are planning to spend $1 million or more over the next three years.

As the technology becomes more exciting and the industry gathers pace, the pressure is on for quantum to deliver. But the voice of skeptics will also grow louder. In the face of those that say quantum computers will never be useful due to their complexity and limited results to date, the question on everyone's mind is, will 2023 be a breakthrough year for quantum computing?

### Technical innovations vs market incumbents

During 2022, we saw the creation of many industry incumbents who used SPACs, IPOs, mergers or corporate sponsorship to build themselves substantial war chests to pursue some serious engineering activity. While these significant scale-up activities will continue, 2023 will also be the year of innovation and possible disruption.

Amongst the big players, new players will emerge with alternative approaches towards quantum computing: Perhaps replacing qubits and gate models with qumodes, using model simulations and quantum annealing models.

The aim of these newcomers will not be to solely achieve universal computing, but rather more specific and useful computation that can be delivered in a shorter timescale. The challenge will be whether these new machines can be applied to something useful and that the industry will care about them in the near term. The quantum supply chain is also developing with component-based suppliers — such as quantum processor vendors — that will shake loose how full-stack systems are built and break the economics of current black box approaches.

Such work will force further discussions about the right and best way to compare and benchmark technologies, performance and the industry.

## Competition for financing

Despite the turmoil in the international financial markets, quantum computing may continue to buck the trend with large funding rounds. Also, 2023 will see an interesting comparison between public and privately owned quantum companies.

Public companies will continue to put their capital to work, but at the cost of the short-term attention of investors and short sellers. While they and the rest of the industry push to meet meaningful and substantial technical milestones, they will have only partial success in shrugging off the short-term pressures to validate the business. It's likely that a race to capture the first market share to meet revenue predictions will ensue.

In the private space, and with a global recession looming, large companies' valuations will likely struggle to compete with previous expectations. This will be countered to an extent by the increasing appetite for deep tech, as well as new, exciting developments. Within the recent glut of new quantum companies, many will struggle, and both successful and less successful companies will be acquired as the big players consolidate. In general, 2023 will likely end with fewer quantum companies than in 2022.

For both public and private quantum companies, it will help when a few make strides toward creating useful cases with near-term quantum computers. In the pursuit of pragmatic value-creation, this will come in many forms — including quantum sensing and comms, quantum-inspired, and hybrid quantum-classical approaches with small-scale systems.

A few successes here will be industry-changing, which will start to bring about a focus that the industry has been waiting for. The consequences will ripple through the entire market.

## Making progress toward fault-tolerant machines

Despite progress on short-term applications, 2023 will not see error correction disappear. Far from it, the holy grail of quantum computing will continue to be building a machine capable of fault tolerance. 2023 may create software or hardware breakthroughs that will show how we're closer than we think, but otherwise, this will continue to be something that is achieved far beyond 2023.

Even though it's everything to some quantum companies and investors, the future corporate users of quantum computing will largely see it as too far off the time horizon to care much. The exception will be government and anyone else with a significant, long-term interest in cryptography.

However, regardless of those long time horizons, 2023 will define clearer blueprints and timelines for building fault-tolerant quantum computers for the future. Indeed, there is also an outside chance that next year will be the year when quantum rules out the possibility of short-term applications for good, and doubles down on the 7- to 10-year journey towards large-scale fault-tolerant systems.

### Governments, users and HPC

2022 saw the German government conclude the tendering process for some very large quantum computing projects, with one example of a €67m contract for two projects. In 2023, that trend will continue with yet more public procurements for quantum computing.

Those tenders and the fact that they will be run through several of the world's HPC centers will force the quantum computing industry to live up to the rigor of tender requirements, and the delivery obligations which come with it. So long as those tenders are run well, these activities will force up the maturity of the technology, and the companies in this space.

Alongside that, the sophistication of the user community will develop dramatically this year. Expect the launch of several 'industrial challenges' delivered by teams of in-house quantum experts. Again, this increasing maturity will act as a force for good within the industry, helping to create great strides toward the search for concrete applications and roadmaps.

### Geopolitics standing in the way

Geopolitics will continue to shape quantum as it does the rest of the economy; this shaping could reach a fever pitch with the growing separation between the U.S. and China. As the race is on to develop quantum computers to gain a strategic lead in cybersecurity, intelligence operations and the economic industry, expect increasing restrictions to limit technological exchange and increasing impact on supply chains. This will be partially offset through bi and multilateral agreements between nations, although the specter of nationalism will linger.

But how will European and UK companies fare? Many are fearful of being caught up in the middle of the China-U.S. tech competition, and so are urgently designing quantum tools to protect their interests.

### A breakthrough year for quantum

So as we look forward, it's no longer a question of *if* quantum computing will be available *but when*? 2023 may be the year in which some ask — and perhaps even claim *now.* Whereas others will continue to say, *"of course not."*

With more and more companies adopting quantum to explore its potential, we will certainly leave 2023 more aware of the benefits and timeline. This may help companies better understand what their future could look like with quantum.

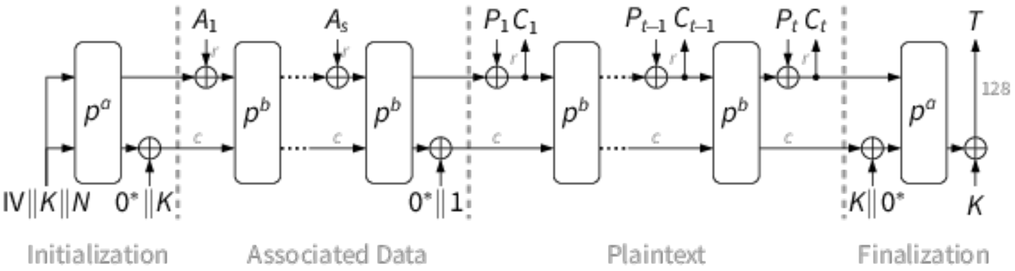
Yet however little we know about what the future holds, one thing is certain: The world will be watching.

# 12.Ascon Algorithms Finalized For Lightweight Cryptography

by Majeed Ahmad
https://www.edn.com/ascon-algorithms-finalized-for-lightweight-cryptography/

The National Institute of Standards and Technology (NIST) has selected a group of cryptographic algorithms to secure the Internet of Things (IoT) devices and the related tiny sensors and actuators. Ascon, a group of cryptographic algorithms, will also serve other miniature devices like medical gadgets, stress detectors inside roads and bridges, and keyless vehicle entry fobs.

NIST will publish the "lightweight cryptography" standard later this year. It'll be targeted at tiny devices that have limited resources and thus demand a compact security implementation. "The Ascon algorithms for lightweight cryptography will cover devices with resource constraints," said NIST computer scientist Kerry McKay.



Ascon algorithms have withstood years of examination by cryptographers.

Several years ago, NIST announced a development program to determine the strongest and most efficient lightweight algorithms, first communicating with industry and other organizations to understand the needs. In 2018, it requested potential solutions from the cryptography community and received 57 submissions. Next, McKay and mathematician Meltem Sönmez Turan carried out a multi-round public review process and selected 10 finalists.

Finally, Ascon became the winner for its algorithm's performance and flexibility in terms of speed, size, and energy use. Ascon—developed in 2014 by a team of cryptographers from Graz University of Technology, Infineon Technologies, Lamarr Security Research, and Radboud University—is currently available in seven variants.

## Ascon's lightweight cryptography variants

According to McKay, Ascon's two variants or tasks are among the most important in lightweight cryptography: authenticated encryption with associated data (AEAD) and hashing. AEAD—besides protecting the the confidentiality of a message—allows additional information like the header of a message or a device's IP address to be included without being encrypted. In lightweight cryptography, it can be used in vehicle-to-vehicle communications. It can also help prevent the counterfeiting of messages exchanged with the RFID tags that often help track packages in warehouses.

On the other hand, hashing creates a short digital fingerprint of a message that enables a recipient to determine whether the message has changed. It can be used to check whether a software update is appropriate or has been downloaded correctly.

Here, it's worth mentioning that the the most efficient NIST-approved technique for AEAD is the Advanced Encryption Standard (AES), while SHA-256 is widely used for hashing. However, as McKay clarified, the goal of this project is not to replace AES or hash standards. “NIST still recommends their use on devices that don’t have the resource constraints that these new algorithms address.”

McKay added that the new algorithms are also not intended to be used for post-quantum encryption, another current concern of the cryptography community that NIST is addressing. “Post-quantum encryption is primarily important for long-term secrets that need to be protected for years,” she said. “In contrast, lightweight cryptography is generally important for more ephemeral secrets.”

# 13.How Quantum Computing Can Solve Supply Chain Challenges

by Marcus Law
https://supplychaindigital.com/pr_newswire/how-quantum-computing-can-solve-supply-chain-challenges

Programming techniques could help solve massive quantum optimisation problems, with the end result of helping the world overcome supply chain challenges

The ongoing Russo-Ukrainian conflict and the COVID-19 pandemic have shown how vulnerable global supply chains can be. But new research in quantum computing at Sandia National Laboratories is moving science closer to being able to overcome supply-chain challenges and restore global security during future periods of unrest.

Capable of solving problems up to 100 million times faster than traditional computers, quantum computing has the potential to comprehensively speed up processes on a monumental scale.

Alicia Magann, a Truman Fellow at Sandia, has led the development of a new way to design programs on quantum computers, which she and her team think could be especially useful for solving massive optimisation problems at a future point when quantum technology becomes more mature.

“Reconfiguring the supply chain on short notice is an exceptionally difficult optimisation problem, which restricts the agility of global trade,” she commented.

Optimisation algorithms help industries perform tasks like coordinating trucking routes or managing financial assets. These problems are generally difficult to work out, Magann said, and as the number of variables increases, finding good solutions becomes harder.

One of the potential long-term solutions to solving complex optimisation problems is to use quantum computers, an emerging technology that experts believe will be able to find answers to some problems much faster than supercomputers.

But building quantum computing technology is only one of the challenges.

“There’s also this other question of: Here’s a quantum computer — how do I actually program this thing? How do I use it?” Magann said.

## Better solutions needed for large-scale quantum applications

As explained in a paper by IBM, supply chain and logistics professionals have been stretched thin over the past several years, with an increasing amount of uncertainty – from labour shortages to extreme weather, to pandemic-fueled changes in supply and demand – increasing logistics complexity exponentially.

“The solution to this complexity requires a broader perspective,” IBM says. “Silo-based, function-based, or even enterprise-wide optimizations no longer provide the cure for supply chain and logistics challenges. Instead, businesses need supply chain optimizations that account for the full complexity of the entire ecosystem. They need quantum logistics.”

Researchers around the world are actively developing algorithms for large-scale optimisations on future technologies, with the hope that these programs could help industries manage limited resources more effectively and pivot operations more quickly in the face of rapid changes to the labour market, supplies of raw materials or other logistics.

Mohan Sarovar, the principal investigator on Sandia’s project, said: “It’s very difficult to come up with quantum algorithms. One of the big reasons for this, apart from quantum computing being very unintuitive, is that we have very few general frameworks for developing quantum algorithms.”

New quantum framework to solve intricate supply chain problems

According to their research, the Sandia team succeeded in greatly reducing the role of classical computing. With the new framework, FALQON (Feedback-based Algorithm for Quantum Optimization), the classical computer does not do any optimisation. It only needs the computational power of a calculator, letting the quantum computer do all the heavy lifting and theoretically allowing it to work on much more complicated problems, like how to efficiently reroute a shipping fleet when a major port suddenly closes.

“After I run the first layer of the algorithm, I measure the qubits and get some information from them,” Magann said. “I feed that information back to my algorithm and use that to define the second layer. I then run the second layer, measure the qubits again, feed that information back for the third layer, and so on and so forth.”

Until quantum computers become more powerful, the framework is largely a theoretical tool that can only be tested on problems classical computers can already solve. However, the team at Sandia believes the framework shows great potential for formulating useful algorithms for the medium-to-large-scale quantum computers of the future.

# 14.National Cybersecurity Strategy To Include Guidance On Post-Quantum Cryptography

by Naomi Cooper
https://executivegov.com/2023/02/national-cyber-strategy-to-include-guidance-on-post-quantum-cryptography/

The forthcoming National Cybersecurity Strategy from the Office of the National Cyber Director will include guidance on standardizing quantum-resistant cryptography, NextGov reported Wednesday.

Dylan Presman, director of budget and assessment at the Office of the National Cyber Director, confirmed the inclusion of the guidance in the framework and said that the office “will take a strong stand” on the transition of networks to post-quantum cryptographic standards.

Speaking during an Advanced Technology Academic Research Center discussion, Presman acknowledged the transformational qualities and opportunities of quantum computers but noted that there are steps needed to be taken to secure U.S. networks and systems from adversarial threats.

According to Presman, organizations looking to transition to post-quantum cryptography must first conduct a thorough inventory of data and technologies used across the enterprise.

He said there are automation tools available in the market to assist government and commercial institutions in preparing for the transition.

# 15.Preparing For Post-Quantum In 10 Steps

by Johannes Lintzen
https://www.information-age.com/preparing-for-post-quantum-in-10-steps-123501654/

With post-quantum technology having the potential to trigger a new wave of cyber threats, we identify 10 steps that organisations should take to prepare.

The security implications of post-quantum technology are legitimate cause for concern. Around the world, corporations and nation-states are pouring millions of dollars into developing quantum computing technology. In response, governments and supranational organisations are sounding the alarm and readying themselves for a new era of cyber threats. Yet, the prospect of such threats should cause neither panic nor paralysis. As with all disruptive technologies, preparation is the best defence.

Concerns about protecting data and assets from post-quantum threats are best assuaged through so-called ‘cryptographic agility’. Cryptographically agile organisations can shift gears quickly, switching out their original encryption method or cryptographic primitive (the building blocks of higher-level cryptographic algorithms), without disrupting their overall system infrastructure. This will be an important attribute for any organisation looking to achieve quantum readiness, as quantum algorithms will develop and update as cryptographic research matures in line with technical advances.

The following ten-step checklist is a useful jumping-off point for security teams seeking to determine their organisation’s level of readiness for Post-Quantum Cryptography (PQC), and create an effective strategy to realise true cryptographic agility.

## Ten steps toward post-quantum readiness

### Assess

Like preparing for any other security overhaul, the road to cryptographic agility begins with a thorough analysis of the organisation’s environment, to determine exactly what you’re working with, where the gaps are, and what needs to be done next:

1. Take stock of your entire security strategy.
2. What cryptographic tools do you use?

3. Who has control over them?
4. What is the lifecycle management policy?
5. Create a comprehensive inventory of your cryptographic tools.

As part of the assessment process, organisations must identify all of the systems currently using cryptographic technologies for any function, as well as any cybersecurity and data security standards in place that will need to be updated in line with post-quantum requirements.

### Prioritise

Data currently encrypted by methods based on classical cryptography can be accessed and stored by bad actors until they obtain quantum technology, in a move known as an “Store now, decrypt later” (SNDL) attack. This means that organisations warehousing data with a long shelf life must be particularly aware of this threat, and make plans that prioritise valuable data with a long shelf-life:

6. Determine what is your most valuable data.
7. Which data has the longest shelf life?

### Plan for action

Creating and adopting a cryptographically agile approach allows organisations to future-proof their security strategy by providing the mechanism to address potential threats quickly and effectively as they appear:

8. Make plans to migrate the most valuable data, together with the data with the longest shelf life, to PQC first.
9. Prepare to follow NIST guidelines for PQC algorithms, but be prepared to adopt changes on the fly.
10. Adopt a cryptographically agile strategy.

While each of these steps is critical to achieving cryptographic agility and preparing a strategy for post-quantum readiness, they can be challenging without the right support. Consider finding an expert in cryptographic security solutions to help your organisation develop a strategy to achieve cryptographic agility.

# 16.Project Combines Quantum Cryptography And Li-Fi

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/project-combines-quantum-cryptography-and-li-fi/

Modern quantum technology opens up many new areas of application. But it also harbours risks. Due to their enormous computing power, quantum computers, could undermine even the most modern data encryption methods. To forestall this scenario, several partners led by KEEQuant GmbH are developing a new approach to secure optical data transmission in wireless networks using light and quantum keys. The “QuINSiDa” project is funded by the German Federal Ministry of Education and Research BMBF with a sum of 2 million euros

In the project, researchers are developing technologies for wireless quantum communication between multiple devices within a room.

Currently, many quantum technology innovations are on cusp of being realised. In addition to quantum computers, quantum imaging and quantum clocks, developments are focusing primarily on quantum communication and quantum encryption for secure and private data communication. Here, classical encryption approaches based on computational complexity are to be replaced by novel quantum key distribution approaches in combination with post-quantum cryptography. This type of encryption cannot be cracked even with arbitrary time and computational power. Since existing cryptography is already threatened in the near future by the ever-increasing computational power of quantum computers, approaches must be developed in time to prevent an insecure transition period.

Previous research has focused on long-distance secure data communication for applications in the global data infrastructure, for networking government or military facilities, or for information exchange with satellites. However, the connections to the end user on the last kilometer have so far still been served by classical technologies and thus remain vulnerable to attack. To prevent this in the future, the project "QuINSiDa – Quantum-based Infrastructure Networks for Safety-critical Wireless Data Communication" was launched. The project, funded by the BMBF, has a planned duration from 01.09.2022 to 31.08.2025.

## Linking Li-Fi technology and quantum cryptography

Li-Fi technology allows users to network with each other over short distances using optical signals. Compared to the familiar Wi-Fi technology, which is based on radio waves, the optical signals do not penetrate walls and can therefore be designed for a defined area. Li-Fi technology also allows full utilization of the available spectral data bandwidth in this area without interference from outside.

Independent of this, quantum cryptography is being advanced worldwide. In specific, this involves quantum key distribution (QKD), which makes it possible to distribute a cryptographic key whose security can be proven from an information-theoretic point of view. This contrasts with existing cryptographic techniques, where security is based on computational complexity and is compromised by emerging quantum computers.

In quantum key distribution, quantum states in the form of light are prepared and exchanged between participants in the network when the keys are generated. When the quantum states are received, they are measured and post-processed to produce keys that are identical on both sides but secret to an attacker. The QuINSiDa project is the first to combine both technologies into a "QKD over Li-Fi" system. This makes it possible to carry QKD, which until now has typically been thought of more in a building-to-building scenario, all the way to the end user.

"The intention of the project is to demonstrate a quantum-based data communication network that wirelessly and flexibly connects multiple end users to a secure backbone infrastructure or which can be deployed separately as a secure campus network," says Dr. Imran Khan Managing Director of KEEQuant GmbH. The idea is to use a flexible wireless data communication network in a point-to-multipoint scenario to simultaneously secure the individual communication channels based on quantum keys.

## Technology application

In contrast to radio-based approaches, the use of an optical communication network offers the advantage that every participant who registers in the optical wireless communication channel (Li-Fi channel) is also visible to the quantum channel. This ensures that secure key exchange can occur. Different wavelengths of light are used to separate the Li-Fi channel and the quantum channel. This separation can be optimized by the receiver by using appropriate optical filtering against interference.

The concept of a quantum-based infrastructure network for safety-critical wireless data communication is a completely new interdisciplinary approach that has not yet been presented in scientific publications or in current market solutions. The approach will be investigated by the project partners primarily with respect to security-critical applications, such as equipment for public utilities, including banks, hospitals, utilities, public services, telecommunications nodes, and government facilities. Here, special attention will be paid to the security of the overall system with simultaneous, interdisciplinary integration of network management software, classical cryptography (keyword: post-quantum cryptography), QKD technology and Li-Fi technology. At the same time, considering the background of technological sovereignty, the project is of social importance for Germany as a business location.

At the end of the project, a corresponding demonstration of the overall system is planned, which will bring the technologies together in a network and thus enable previously unexplored and unachieved use cases. Following the project, these will be exploited by the participating companies and incorporated into safety-critical applications. Due to the end-user focus, a broad application and thus a very large market potential and innovation potential can be identified. In addition, the drastic cost reduction in QKD that will arise in the next few years due to production in medium quantities will allow broader market penetration.

Furthermore, the interdisciplinary networking between the different communities (QKD, optics, telecommunication, security) leads to a seamless integration of the novel technologies into existing security technologies. This makes it easy for end users to adopt the technology into existing infrastructure.

# 17.Your RSA Security Is On Its Last Legs. What’s Next?

**by Vincent Berk**
https://www.forbes.com/sites/forbestechcouncil/2023/02/13/your-rsa-security-is-on-its-last-legs-whats-next/?sh=76e910e0719c

A recent paper from Chinese researchers claiming that they can break traditional RSA encryption initially sparked an uproar. Calmer voices have cited flaws in the research, so the panic has died down a bit. Yet it portends a future that, in reality, may not be too far away.

RSA and the Diffie-Hellman key exchange are two closely related mathematical cryptographic methods that underlie all modern data encryption used today. So what happens when RSA is completely broken, when cryptography as we’ve known it for the last 40-plus years is defeated?

It’s next to impossible to quantify the risk and the impact of that day. But we must prepare for it.

One of the things that make that preparation difficult is the way in which current cryptography is integrated into computing systems.

Cryptography has traditionally been treated as a stalwart and trustworthy part of software and hardware. Cryptographic libraries get compiled directly into software applications, operating systems and server containers. It’s baked blindly into each and every application, not shared across the hundreds or even thousands of applications deployed in a global organization and nigh on impossible to maintain consistently.

Even a global corporate chief information security officer (CISO) or infrastructure and networking leader has virtually no control over this. For the most part, they can't choose which cryptographic security technology is used. And there's little they can do if it's broken. They have to wait for the application or hardware provider to send over an update.

The entire concept of cryptography has been abstracted away. CISOs have no idea what cryptography is being used, how it's being used, or if what they want to be encrypted is actually encrypted. They are forced to just accept the crypto on their servers, their VPNs, their video conferencing app—without even knowing what they have and, thus, what the risks may be in the event of a failure.

The really scary part is that while a quantum computer (such as the one referenced in the Chinese paper) gets all the headlines, a bug in the library you are using today may pose just as big a threat—and sooner. Look no further than the recent Java 15+ ECDSA bug or the all-too-painful Heartbleed for examples.

But you know what is really the kicker? Each cryptographic environment is based on one single algorithm, one certificate or password, one implementation. It's a monoculture of security—the literal definition of putting all your eggs in one basket.

In contrast, multiple hard drives are used to create an array with redundancies across systems or locations. Out of these arrays, you might build cloud storage, which can be distributed across multiple data centers, also creating redundancy and spreading risk.

In cryptography, however, we accept this monoculture. All it takes is one bug, one quantum algorithm, one malicious insider, and the security will fail.

Some may take solace in emerging "quantum-resistant" cryptography algorithms coming out of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). The thinking is that you can swap out a new crypto, replacing RSA in case it is broken.

But the risk with that approach is that the algorithms are new. In fact, one of the NIST finalist algorithms was hacked in an hour using a traditional computer. We simply don't know what's already been broken that we just haven't discovered yet.

So what can security professionals do today to offset the threat of a catastrophic cryptography failure?

1. **Commit to cryptography:** Create a "center of excellence" and staff it with subject-matter experts responsible for knowing all there is to know about crypto in the organization. Build a complete inventory of crypto and keys used and stored in the enterprise. Identify what protocols and algorithms are used by what servers and software. Only by understanding your situation can you accurately judge the risk.

2. **Demand transparency:** You need to add the requirements for crypto agility and a software bill of materials in your purchasing process to provide visibility across systems and knowledge of the constituent components of products that perhaps weren't built by the vendor you're buying it from. Crypto agility and this "parts list" gives you critical information to inform purchases and threats and the flexibility to make changes when and where you need to.

3. **Plan your cryptographic policy:** To achieve cryptographic policy management, you must start with a migration strategy that works for your business or operational needs. For example, what are the top priorities for migration—infrastructure, desktop, then application? Define how to roll out crypto management, starting with the highest-risk area. And establish a protocol for what to do when cryptography is defeated.

Security professionals can no longer afford to just "trust" cryptography or to rely on a false sense of security that there is no fault with their cryptography.

Working under the assumption that your cryptography has already been hacked, it's time to take an enterprise approach to crypto management. You must build an ecosystem where monocultures in algorithms and their implementations can be diversified, made more agile and managed through policy.

Only then can you be confident that you have built a dependable cryptographic system that can withstand future attacks.

# 18.New Report Shows Quantum Technologies Thriving In Europe

by James Dargan
https://thequantuminsider.com/2023/02/10/new-report-shows-quantum-technologies-thriving-in-europe/

The new study published by the European Commission called "*Taking the lead in the quantum revolution*" shows Europe's quantum technology ecosystem is thriving with a suite of solutions being developed by projects, start-ups, and spin-offs for a number of applications, including sensing, communication, and computation.

The driving force behind many of the continent's quantum technology breakthroughs since 2018 is the Quantum Flagship—Europe's €1 billion, ten-year research and innovation program, the report reveals.

## Growth from Ramp-Up Phase

Since the initial four-year 'ramp-up' phase (2018–2021) began, Europe's 1500 quantum scientists across 236 organizations filed 105 patents (with 64 already granted) and published 1313 scientific papers (with a further 223 under review).

Investment in quantum technologies has been vital in establishing strong growth within the sector. According to the report, during the 'ramp-up' phase, the European Commission invested €150 million to support 24 consortia involving leading research institutions and companies.

This growth phase was complemented by the QuantERA project — a network of 39 public Research Funding Organizations (RFOs) supporting research and innovation in Quantum Technologies — which leveraged a combined €88.9 million. These combined activities helped establish 25 start-ups and spin-offs which are working to commercialize communication, computation, simulation, sensing, and metrology solutions.

The report notes the Flagship's efforts to move advanced quantum technologies from the laboratory to industry with a suite of prototypes and products ready for market.

## Highlights of the Quantum Flagship

- **Quantum Computing —** the Flagship's researchers have been investigating the most promising scalable quantum computing platforms (superconducting, trapped ions, silicon) to assemble working quantum processors for each approach.

  OPENSUPERQ is building a globally competitive quantum computer system based on superconducting integrated circuits to outperform classical computers. It will be available at the national research institution, Forschungszentrum Jülich (DE) early 2023. The system is based on integrated electric circuits made from superconducting metals, combining the whole stack of necessary hardware and software components.

The OPENSUPERQ quantum computer has measurement and cryogenics systems that can hold 100 qubits with state-of-the-art errors in gate operations and has a processor which has already been used for a global first in quantum error correction with 17 qubits.

Meanwhile, the Flagship's researchers at the AQTION project have been developing an ion-trap quantum computer—a system using ions trapped by electric fields and manipulated with lasers.

- **Quantum Internet —** Researchers in the Flagship's Quantum Internet Alliance (QIA) project have taken the first step into offering a fundamentally new quantum internet technology by enabling quantum communication between any two points on Earth.

QIA has created a network around three quantum nodes 1.3 km apart, enabling the end-to-end delivery of qubits between any two-network nodes, one qubit at a time.

The project has connected two quantum processors through an intermediate node, establishing shared entanglement between multiple stand-alone quantum nodes.

**Quantum Sensing and Metrology—**The Flagship's ASTERIQS H2020 project has developed some of the world's most advanced quantum sensors based on nitrogen-vacancy (NV) centres in ultra-pure diamonds, which will make lightweight and efficient batteries possible for wide-spread use of electric cars in place of fuel cars.

Metaboliqs is currently developing promising approaches for improving medical imaging diagnostics and spectroscopy by using more precise, practical, and efficient nuclear magnetic resonance (NMR).

The quantum microscope developed by Metaboliqs will provide researchers with a unique tool that significantly advances cell analysis and creates new opportunities for in vitro diagnostics and medical research.

## European Quantum Outlook

The report finds that the initial ramp-up phase has established strong foundations upon which Europe can build its globally-competitive quantum ecosystem of SMEs, corporations, investors, and leading researchers.

The success of the Flagship's ramp-up phase has enabled significant investment from major national quantum initiatives, creating funding comparable to that already committed by the Flagship (€2 billion in Germany, €1.8 billion in France, and €670 million in the Netherlands). The authors note that coordinating research at national and European levels is more critical than ever, given that no single country can carry out the complex endeavors required to develop quantum technologies by itself.

At the time of publication, the first quantum computers are being acquired and deployed in EuroHPC. Similarly, the Flagship continues to mature other qubit approaches so that they can be sufficiently deployed over the coming years. As the Flagship moves into its second era, it will continue to mature its quantum computers and develop the most promising new technologies, such as photonic quantum computing.

Several projects have secured a second phase of European funding to establish, maintain and implement a strategic research roadmap in targeted quantum pillars, such as the EuroQCI and EuroQCS projects launched to develop quantum infrastructures.

At the end of 2022, updates to the Strategic Research and Industry Agenda (SRIA) and the Strategic Industry Roadmap (SIR) from the Quantum Industry Consortium (QuIC) were published based on the Strategic Research Agenda (SRA). These updates introduced the industrial perspectives for quantum technologies and the Flagship's links to other quantum initiatives, such as the European High Performance Computing Joint Undertaking (EuroHPC), the European Quantum Communication Infrastructure initiative (EuroQCI), and the European Chips Act.

A new Strategic Research and Industry Agenda will be published in 2023, reflecting the Flagship's progress so far and setting goals for its future. The Commission will continue to support the Flagship until 2027 with at least €500 million in funding from Horizon Europe.

# 19.Post-Quantum Readiness: Is Your Head Of It A Hydra?

by Tracy Levine
https://www.forbes.com/sites/forbestechcouncil/2023/02/10/post-quantum-readiness-is-your-head-of-it-a-hydra/?sh=4598dc3a6a7b

In Greek and Roman mythology, the dreaded Hydra was an insurmountable challenge; no matter how many heads were cut off, two more would instantly sprout in its place. This same sense of perpetual struggle is felt by modern-day CISOs attempting to engage their head of IT on post-quantum cybersecurity—a seemingly Herculean task that constantly regenerates itself regardless of the effort expended.

Whenever the CISO brings up the topic of post-quantum cybersecurity and attempts to educate and advocate for post-quantum cryptography (PQC), the head of IT may brush off the concerns and move on to other priorities. For example, the head of IT may propose traditional cybersecurity measures that address current threats but may not be sufficient to protect against future quantum attacks. Each time the CISO points out the shortcomings of these solutions, the head of IT may propose new solutions, such as endpoint monitoring or air-gapped cold vaults, but they may still not address the post-quantum threat. This can make it feel like there are always more heads to cut off, and the CISO is constantly battling a never-ending problem.

## The Tragic Story Of The IT Hydra

Once upon a time, in a kingdom far, far away, there lived a mighty nine-headed IT water snake named Hydra. Hydra was known throughout the land for overseeing advanced technology and its great power, and many relied on it to protect the kingdom's sensitive information.

One day, a group of wise sages came to the kingdom and proposed a new way of securing the kingdom's communications using a new type of encryption called post-quantum cryptography. They explained that PQC was much more secure than the traditional methods and would protect the kingdom's secrets from even the most powerful adversaries—quantum computing attacks.

However, Hydra was not impressed. "We are the most advanced IT in the land," it declared. "I do not need this newfangled encryption to protect us."

The sages warned that without PQC, the kingdom would be vulnerable to quantum computing attacks, but Hydra paid no heed.

Seeing the cost and effort of implementing PQC, Hydra went to legal to understand the risks. The legal department of the kingdom told the IT department that they were not liable for any breaches in security as they were using state-of-the-art technology mandated and required at the time. And so, with this legal backing, Hydra refused to move to PQC encryption.

Sure enough, a powerful enemy soon appeared on the horizon, armed with the latest technology that could easily break the traditional encryption methods. The enemy quickly breached the kingdom's defenses and captured the kingdom's secrets. The people of the land were outraged and blamed Hydra for their plight.

Realizing its mistake, Hydra tried to make amends and protect the kingdom with its strength, lawyers and cybersecurity insurance, but it was not enough, and it was too late. The damage was already done, and the kingdom was left in ruins.

## Moral Of The Story

Legal protection can be a false sense of security, and IT departments must take their duty of care seriously. It's important to stay informed and adapt to changes in order to protect oneself and one's kingdom, even if it comes at a cost.

In today's fast-paced business world, it's crucial for companies to stay ahead of the curve when it comes to post-quantum security. One of the most pressing issues facing companies today is the rise of "steal now and decrypt later.”

As cybercrime continues to grow, the reality of modern data theft is becoming ever clearer: Losing valuable information and intellectual property can be devastating. With technology making it easier for hackers to save stolen assets cheaply in the cloud until quantum computing encryption-cracking solutions become available, organizations need a robust security strategy more than ever before if they hope to prevent irreparable damage.

So, how do you know if your head of IT is a "Hydra" when it comes to PQC?

It's simple. If your company has not discussed the NSA Advisory titled "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," you may have a Hydra.

The NSA Advisory document outlines the final standards and timelines for transitioning to post-quantum cryptography. Failure to do so puts your company at risk of becoming a prime target for cyberattacks. Don't wait until it's too late—take the necessary steps to ensure your company is prepared for the transition to PQC before the initial deadlines pass. Don't be the last adopter; be a leader in the industry by proactively addressing this critical issue.

Companies should already be taking the following steps to meet the NSA Advisory timeline for transitioning to PQC.

- **Software and firmware signing:** Companies should immediately begin transitioning to CNSA 2.0, a set of software and firmware signing guidelines.
- **Traditional networking equipment:** Companies should have a roadmap to transition the majority of their traditional networking equipment, such as virtual private networks (VPNs) and routers, to

PQC by 2026.

- **Operating systems:** Companies should have a roadmap to transition the majority of their operating systems to PQC by 2027.

It's worth noting that these steps are not only recommended but also required by some regulated industries such as banking, finance, and government since they are critical systems, and it's required to protect the sensitive information that these systems hold.

Companies must take PQC seriously and take the necessary steps to protect themselves from post-quantum attacks. Companies that don't take PQC seriously risk falling victim to a devastating data breach and potentially losing the trust of their customers, partners, and shareholders. It's time to take a stand against the "Hydra" mentality and ensure that your company is protected against the current threat of quantum computing attacks presented by "steal now and decrypt later."

# 20.Quantum Breakthrough Could Revolutionise Computing

by Pallab Ghosh
https://www.bbc.com/news/science-environment-64492456

Scientists have come a step closer to making multi-tasking 'quantum' computers, far more powerful than even today's most advanced supercomputers.

Quantum computers make use of the weird qualities of sub-atomic particles.

So-called quantum particles can be in two places at the same time and also strangely connected even though they are millions of miles apart.

A Sussex University team transferred quantum information between computer chips at record speeds and accuracy.

Computer scientists have been trying to make an effective quantum computer for more than 20 years. Firms such as Google, IBM and Microsoft have developed simple machines. But, according to Prof Winfried Hensinger, who led the research at Sussex University, the new development paves the way for systems that can solve complex real world problems that the best computers we have today are incapable of.

“Right now we have quantum computers with very simple microchips," he said. "What we have achieved here is the ability to realise extremely powerful quantum computers capable of solving some of the most important problems for industries and society.”

Currently, computers solve problems in a simple linear way, one calculation at a time.

In the quantum realm, particles can be in two places at the same time and researchers want to harness this property to develop computers that can do multiple calculations all at the same time.

Quantum particles can also be millions of miles apart and be strangely connected, mirroring each other's actions instantaneously. Again, that could also be used to develop much more powerful computers.

One stumbling block has been the need to transfer quantum information between chips quickly and reliably: the information degrades, and errors are introduced.

But Prof Hensinger's team has made a breakthrough, published in the journal Nature Communications, which may have overcome that obstacle.

The team developed a system able to transport information from one chip to another with a reliability of 99.999993% at record speeds. That, say the researchers, shows that in principle chips could be slotted together to make a more powerful quantum computer.

Prof Michael Cuthbert, who is the director of the newly established National Quantum Computing Centre in Didcot, Oxfordshire and is independent of the Sussex research group described the development as a "really important enabling step". But he said that more work was needed to develop practical systems.

"To build the type of quantum computer you need in the future, you start off by connecting chips that are the size of your thumbnail until you get something the size of a dinner plate. The Sussex group has shown you can have the stability and speed for that step.

"But then you need a mechanism to connect these dinner plates together to scale up a machine, potentially as large as a football pitch, in order to carry out realistic and useful computations, and the technology for communications for that scale is not yet available."

PhD student Sahra Kulmiya, who carried out the Sussex experiment, says that the team are ready for the challenge to take the technology to the next level.

"It is not just solely a physics problem anymore," she told BBC News.

"It is an engineering problem, a computer science problem and also a mathematical problem.

"It is really difficult to say how close we are to the realisation of quantum computing, but I'm optimistic in how it can become relevant to us in our everyday lives."

One of the UK's leading engineering firms, Rolls Royce, is also optimistic about the technology. It is working with the Sussex researchers to develop machines that could help them design even better jet engines.

Powerful supercomputers are used to model the flow of air in simulations to test out new designs of aircraft engines.

## Transforming engineering

A quantum computer could in principle track the airflow with even greater accuracy, and do so really quickly, according to Prof Leigh Lapworth, who is leading the development of quantum computing for Rolls-Royce.

"Quantum computers would be able to do calculations that we can't currently do and others that would take many months or years. The potential of doing those in days would just transform our design systems and lead to even better engines."

The technology could potentially also be used to design drugs more quickly by accurately simulating their chemical reactions, a calculation too difficult for current supercomputers. They could also provide even more accurate systems to forecast weather and project the impact of climate change.

Prof Hensinger said he first had the idea of developing a quantum computer more than 20 years ago.

"People rolled their eyes and said: 'it's impossible'."

"And when people tell me something can't be done, I just love to try. So I have spent the past 20 years removing the barriers one by one to a point where one can now really build a practical quantum computer."

# 21.IBM's Vision For Security In The Quantum Era

by Charles King
https://www.eweek.com/security/ibm-security-quantum-era/

Enterprise technology solutions are predicated on the knowledge that large scale businesses face continual, often evolving challenges. Most enterprise IT vendors' offerings and services are designed to help clients successfully address existing problematic issues and digital transformation challenges. The best vendors have the foresight, skills and expertise to help enterprises effectively prepare for ever greater difficulties that lie just over the horizon.

A recent report from IBM's Institute for Business Value (IBV), Security in the Quantum Era offers insights into how this process works. The report examines the potentially catastrophic dangers posed by cybercriminals, rogue states and other bad actors that have access to quantum-level tools. It also discusses what IBM is doing to address those issues and help enterprises secure their IT assets and infrastructures against quantum cyberthreats.

## IBM's Security Focus for the Quantum Sector

IBM has been proactive in developing a host of advanced security offerings, including a suite of IBM Quantum Safe services that are designed to be resistant to quantum-based encryption cracking techniques. Those services are available for the IBM z16 mainframe launched last April, the industry's first quantum-safe enterprise system.

In addition, IBM has spent years building a global team of top cryptography experts to spearhead quantum-safe schemes and preparation plans. The company contributed to developing three of the four algorithms chosen by the National Institute for Standards and Technology (NIST) for post-quantum cryptography standardization and was also a founding member of the GSMA Post-Quantum Telco Network Taskforce.

## Benefits and Dangers of Quantum Computing

The IBV report begins with a simple premise: "Quantum computing is evolving from the fantastical to the feasible."

On the upside, emerging quantum solutions could help solve intractable problems in areas like machine learning, materials science, pharmaceutical research and process optimization. If that future comes to pass, the potential scientific, social and business benefits are enormous and well worth pursuing.

However, like any technology, quantum tools can be leveraged for good or ill. Regarding that danger, the

IBV report notes that in the wrong hands “quantum computing poses an existential risk to the classical encryption protocols that enable virtually all digital transactions.”

As a result, commonplace trusted data encryption mechanisms such as RSA and ECC public-key cryptography (PKC) could be vulnerable, endangering organizations’ information and financial assets.

As the World Economic Forum stated last August, “Considering that the digital economy is estimated to be worth $20.8 trillion by 2025, the repercussions could be staggering.”

Another factor in this scenario is the long-term value of many forms of information, including data related to national security, business strategy, intellectual property, public infrastructure, medical records and product development. The IBV report suggests that those assets are potentially already subject to exfiltration in so-called “harvest now, decrypt later” attacks, with the intention of monetizing data once quantum decryption solutions are viable.

For organizations ranging from large enterprises to government agencies and entities to public utilities to telecommunications providers, preparing for future cyber-attacks backed with quantum-level cryptographic tools is vitally important.

Building “Quantum-Safe” Cryptography Solutions

What does the IBV report suggest enterprises should do to address these dangers?

- **Prepare for potential quantum threats** by educating teams on quantum-safe cryptography and demonstrate how businesses can identify achievable near and long-term cryptographic goals.

- **Discover potential vulnerabilities** by using quantum-safe cryptographic assessments, including how to develop and deploy a successful ecosystem for a common approach to data governance.

- **Transform business operations** by performing analyses that can spot cryptographic dependencies between business-critical systems, thus leaving data vulnerable.

- **Observe the threat landscape** by developing a dashboard to promote visibility and assessment.

## Final Analysis

IBM’s work in quantum-safe offerings and services, along with its continuing investments in advanced security development, show the company doing what it does best. While many enterprise IT vendors tend to compartmentalize product teams and creation, IBM is highly focused on integrating software, infrastructure, data analytics and AI into workable new business solutions and services. Those are crucial to the thousands of enterprises that look to the company for help solving existing business-critical problems.

Just as importantly, IBM’s pursuit of next generation technologies is designed to explore new business opportunities and concerns. The company has been a leading light in commercial quantum system development. It seems likely that the insights it gleaned along the way were foundational to the Quantum-Safe services available with the new generation IBM z16.

The conclusions offered in the IBV’s new Security in the Quantum Era report suggest that the company is acting as it has so often in the past. In essence, IBM is using its considerable investments, insights and inventions to help enterprise customers understand, prepare for and successfully weather future changes and challenges.

# 22. Companies Consider Post-Quantum Cryptography Options

by James Tyrrell
https://techhq.com/2023/02/companies-consider-post-quantum-cryptography-options/

Doing nothing is a bad strategy. But firms can protect their data by considering post-quantum cryptography options and running simulations.

Getting to grips with post-quantum cryptography can quickly turn a stroll into a mountain climb. Understanding how superposition, interference, and entanglement – three key properties that make quantum bits (qubits) different from their classical cousins – will impact data security isn't straightforward. But reframing the scenario can help to shed more light on why companies need to start thinking about their post-quantum cryptography options today.

## Risk management exercise

The topic boils down to risk management and a question of how firms choose to handle the process. "Most agencies put 2030 as the tipping point, from a risk perspective," Nils Gerhardt – CTO at **Utimaco**, a cybersecurity solutions provider with offices in Aachen, Germany, and California, US – told *TechHQ*. "But if you have data that you want to protect, you need to start now."

Driving the transition from current data encryption algorithms to post-quantum cryptography options is a fear that quantum computers could solve the mathematical problems that support today's web security. And it's not just about securing internet traffic. Data storage, firmware signing, and even blockchain-based systems (which use private keys to sign digital ledger transactions) could all be impacted.

As Gerhardt highlights, nobody is sure exactly when quantum computers will gain the capacity – thanks to advances in error correction and increasing numbers of available qubits – to break encryption schemes such as RSA. The cryptography standard (named after its inventors: Ron **R**ivest, Adi **S**hamir, and Leonard **A**dlemanis) is widely used for generating public and private key pairs, and creating digital certificates. But there's a whole raft of encryption schemes that could become vulnerable. And the concern in cryptography circles centers around Shor's algorithm, which opens the door to breaking conventional cryptography standards.

Behind the scenes, encryption schemes such as RSA utilize very large numbers, which become exponentially difficult to factor mathematically as they increase in size. And this provides a security barrier. Classical machines struggle to solve even a small RSA combination. For example, **researchers broke an 829 bit RSA key only after months of effort using a giant cluster of machines** that provided an equivalent of 2700 years of computation time. Today, the recommended key length is 2048 bits, and recall that the computational challenge grows exponentially. So our data is still safe, right?

The catch, as mentioned, is Shor's algorithm, which turns an integer-finding problem into a frequency search to determine the period of a function (which is a shortcut to factoring large numbers). And this latter exercise is something that quantum computers can, in principle, do quite easily. And the more qubits, the tougher the problems that can be solved. Today, while **quantum computer developers such as IBM, and others, have roadmaps to scale up to thousands of qubits**, there remain technical issues to overcome. Depending on the quantum computing architecture, qubits may have to be kept at the temperature of outer space, systems are extremely sensitive and present a wide range of engineering challenges.

## Harvest now, decrypt later threat

But these road bumps shouldn't be read as an excuse for companies to delay considering post-quantum cryptography options. Quite the opposite. It's possible that bad actors are harvesting encrypted data today, banking on the prospect of quantum success in the future – a so-called 'harvest now, decrypt later' attack strategy. To defend themselves, firms will need to switch to a new suite of cryptography approaches.

"We need different algorithms for different use cases," Utimaco's Gerhardt points out. "And to be prepared for more frequent changes in cryptography." For example, constrained devices will have limitations on processing power and some applications will need to prioritize response time. International standards organizations, such as NIST in the US, recognize that one algorithm won't fit all use cases. And, through a long-running competition to find suitable post-quantum cryptography algorithms, has narrowed down its selection to a range of candidates, including **CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, and SPHINCS+**.

The first step that companies can take is to understand which classical algorithms are in use across the organization and where systems are deployed. Such analysis will help companies to determine which post-quantum cryptography options will be most suitable for them. And cybersecurity firms offer **simulators that allow developers to run a post-quantum cryptography proof-of-concept**.

Initially, it's likely that hybrid deployments will be the go-to strategy – in other words, solutions that tunnel a combination of conventional and post-quantum cryptography schemes. The approach means that if holes are found in the new algorithms then protection is still afforded by classical data encryption or digital signing methods running in tandem. It can take years of analysis before the cryptography community declares an algorithm to be, most likely, secure.

## Direction of travel

**Security experts have subsequently poured cold water on the claims**, but for a while there was excitement about results reported by security researchers in China – who submitted a paper on **factoring integers up to 48 bits (261980999226229) with 10 superconducting qubits**. The breakthrough, if quantum scientists elsewhere succeed in reproducing the Chinese team's results, would still be some way off solving 2048 bit keys. But the write-up adds weight to concerns that Shor's algorithm could one day pose a problem to classical encryption schemes. In its paper, the Beijing-based group believes – following a quantum resource estimation – that as few as 372 physical qubits could be sufficient to challenge 'simpler' RSA-2048 configurations. And the team comments that noisy intermediate-scale quantum computers could be up to the task in the near future.

Nobody knows for sure when a quantum computer will be capable of breaking today's data encryption schemes and rendering digital signatures untrustworthy. But the direction of travel is crystal clear. And doing nothing is a bad strategy for companies with data and software that must be protected.

# 23.WISeKey's Semiconductors, NFTs, Post Quantum And Blockchain Solutions Secure

# Smart Cities

by Wisekey International Holding SA
https://www.globenewswire.com/news-release/2023/02/08/2603610/0/en/WISeKey-s-Semiconductors-NFTs-Post-Quantum-and-Blockchain-Solutions-Secure-Smart-Cities.html

WISeKey International Holding, a leading cybersecurity, AI and IoT company, announced today that its security chips are being used to protect all sort of IoT devices connecting Smart Cities, such as #drones and their captured images, satellite communications and logistics sensors. These semiconductors, when placed on any object, securely issue NFTs to authenticate and track the object, much like an embedded ePassport, and confirm the identity of the object on the Blockchain ledger.

Smart Cities benefit from the billions of WISeKey's secure chips already embedded in high-tech products and goods to protect data, communication and firmware against cyberattacks. These include routers, modems, traffic lights, 5G equipment, energy smart meters, drones and medical devices, to mention a few.

Smart cities rely on interconnected communication networks, meaning that a security breach on one system can affect the whole city. IoT can help secure smart cities by implementing the following measures:

1. **Automatically updating security software:** By using IoT-powered systems, cities can implement a patch management system that would monitor and automatically update the security protocols of all systems and networks in the city.

2. **Improved perimeter security**: IoT-enabled sensors and cameras can be placed around the city to monitor important locations and provide real-time alerts on potential threats.

3. **Improved traffic flows**: IoT-enabled traffic systems can help to analyze traffic flows and identify any potential security threats quickly.

4. **Automated identity checks**: Advanced biometric systems can automate identity checks and enhance the security of the city's borders.

5. **Improved data management**: IoT-enabled systems can be used to collect, analyze and store data securely, with tight access control and encryption protocols in place.

6. **Enhanced real-time monitoring:** With IoT-enabled systems, cities can monitor their systems in real-time, allowing for faster detection of security breaches and more effective responses.

Post quantum chips can be used to protect smart cities by increasing key exchange speeds, providing greater security against quantum computer attacks, and reducing vulnerability to human error, malicious actors, and system malfunctions. When combined with other existing cybersecurity measures, post quantum chips can significantly strengthen the defenses of smart cities.

In order to make use of post quantum chips, a city's systems must be upgraded to include quantum-resistant encryption algorithms, which can be integrated with existing systems. This would allow for faster, more secure data transmission between different smart city systems. Additionally, post quantum chips can help strengthen network credibility by ensuring that all data transmitted is cryptographically secure and cannot be altered or accessed without the correct key.

Finally, post quantum chip-based systems are designed with an emphasis on resilience, which is key for smart cities that rely on other connected "things" such as sensors, cameras, and software applications. A resilient system can quickly identify and manage errors or address malicious activities, thus keeping a city safe from potential cyber-attacks. The added protection provided by post quantum chips also allows a city to implement more complex cybersecurity measures.

# 24.NIST Selects 'Lightweight Cryptography' Algorithms To Protect Small Devices

by Chad Boutin
https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices

Lightweight electronics, meet the heavyweight champion for protecting your information: Security experts at the National Institute of Standards and Technology (NIST) have announced a victor in their program to find a worthy defender of data generated by small devices. The winner, a group of cryptographic algorithms called Ascon, will be published as NIST's lightweight cryptography standard later in 2023.

The chosen algorithms are designed to protect information created and transmitted by the Internet of Things (IoT), including its myriad tiny sensors and actuators. They are also designed for other miniature technologies such as implanted medical devices, stress detectors inside roads and bridges, and keyless entry fobs for vehicles. Devices like these need "lightweight cryptography" — protection that uses the limited amount of electronic resources they possess. According to NIST computer scientist Kerry McKay, the newly selected algorithms should be appropriate for most forms of tiny tech.

"The world is moving toward using small devices for lots of tasks ranging from sensing to identification to machine control, and because these small devices have limited resources, they need security that has a compact implementation," she said. "These algorithms should cover most devices that have these sorts of resource constraints."

To determine the strongest and most efficient lightweight algorithms, NIST held a development program that took several years, first communicating with industry and other organizations to understand their needs and then requesting potential solutions from the world's cryptography community in 2018. After receiving 57 submissions, McKay and mathematician Meltem Sönmez Turan managed a multi-round public review process in which cryptographers examined and attempted to find weaknesses in the candidates, eventually whittling them down to 10 finalists before selecting the winner.

"We considered a number of criteria to be important," McKay said. "The ability to provide security was paramount, but we also had to consider factors such as a candidate algorithm's performance and flexibility in terms of speed, size and energy use. In the end we made a selection that was a good all-around choice."

Ascon was developed in 2014 by a team of cryptographers from Graz University of Technology, Infineon Technologies, Lamarr Security Research and Radboud University. It was selected in 2019 as the primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition, a sign that Ascon had withstood years of examination by cryptographers — a characteristic the NIST team also valued, McKay said.

There are currently seven members of the Ascon family, some or all of which may become part of NIST's published lightweight cryptography standard. As a family, the variants give a range of functionality that will offer designers options for different tasks. Two of these tasks, McKay said, are among the most important in lightweight cryptography: authenticated encryption with associated data (AEAD) and hashing.

AEAD protects the confidentiality of a message, but it also allows extra information — such as the header of a message, or a device's IP address — to be included without being encrypted. The algorithm ensures that all of the protected data is authentic and has not changed in transit. AEAD can be used in vehicle-to-vehicle communications, and it also can help prevent counterfeiting of messages exchanged with the radio frequency identification (RFID) tags that often help track packages in warehouses.

Hashing creates a short digital fingerprint of a message that allows a recipient to determine whether the message has changed. In lightweight cryptography, hashing might be used to check whether a software update is appropriate or has downloaded correctly.

Currently, the most efficient NIST-approved technique for AEAD is the Advanced Encryption Standard (defined in FIPS 197) used with the Galois/Counter Mode (SP 800-38D), and for hashing, SHA-256 (defined in FIPS 180-4) is widely used. McKay said that these standards remain in effect for general use.

"The goal of this project is not to replace AES or our hash standards," she said. "NIST still recommends their use on devices that don't have the resource constraints that these new algorithms address. There are native instructions in many processors, which support fast, high-throughput implementations. In addition, these algorithms are included in many protocols and should continue to be supported for interoperability purposes."

Neither are the new algorithms intended to be used for post-quantum encryption, another current concern of the cryptography community that NIST is working to address using a similar public review process for potential algorithms.

"One of the Ascon variants offers a measure of resistance to the sort of attack a powerful quantum computer might mount. However, that's not the main goal here," McKay said. "Post-quantum encryption is primarily important for long-term secrets that need to be protected for years. Generally, lightweight cryptography is important for more ephemeral secrets."

The specification of Ascon includes multiple variants, and the finalized standard may not include all of them. The NIST team plans to work with Ascon's designers and the cryptography community to finalize the details of standardization. Additional information may be found on NIST's project website.

# 25.How Quantum Computing Could Affect The Automotive Landscape

by Itay Lidovski
https://www.cpomagazine.com/cyber-security/how-quantum-computing-could-affect-the-automotive-landscape/

## Cryptography and quantum computing

Once considered science fiction, Quantum Computing (QC) appears set to make its entrance in the coming decade. While current Quantum Computers have very limited functionalities, they are very much real, and by some estimations will be broadly used in several industries by the mid-2030s[1][1][2]. Google claims it already possesses a quantum processor capable of quickly performing calculations that were previously only possible in a huge amount of time.

It is not far-fetched to surmise that in the foreseeable future, quantum computers might take an active role in technological applications. At first, only world powers and giant organizations (such as Google, Amazon, etc.) will possess large-scale, fully operational quantum computers, but later even regular users might have access to quantum computing capabilities, possibly via paid cloud services (some QC services with a very limited capacity are already available[2][3]).

The effects of quantum computing on cryptography, and hence cyber security, are dramatic. Shor's algorithm greatly diminishes the number of operations required in order to factorize large numbers, effectively rendering the most popular asymmetric cryptography schemes – RSA and ECC – unsecure. Grover's algorithm significantly reduces the effectiveness of symmetric schemes, such as AES, requiring developers to double the key size to achieve the same level of security. This means that before QC becomes available to potential attackers, systems using RSA or ECC would have to be upgraded to more secure cryptographic schemes (while AES-dependent systems would need to increase the key size). For this reason, we are now witnessing the rise of Post-Quantum Cryptography (PQC) – a group of cryptographic schemes, such as Kyber[3][4] and Falcon[4][5], which are not susceptible to any currently known attacks by QC.

## Why vehicles are highly susceptible to quantum computing risks

Modern vehicles are connected to the outside world in many ways and for a variety of reasons. This trend is expected to increase in the coming years, due to the use of new vehicle technologies, for example, vehicle-to-infrastructure and vehicle-to-vehicle communications. Other than external communications, vehicles also possess various interfaces between the different computerized components inside the vehicle (called electronic control units, or ECUs) – all of which require secure passage of information.

Cryptography is widely used throughout the automotive landscape as a means to secure data confidentiality, as well as to authenticate the identity of its origin. Common examples include downloading a firmware update over-the-air (FOTA), remote engine ignition, connecting personal mobile devices to the infotainment unit, secure boot, power grid transactions during EV charging, fleet management and communications between in-vehicle systems.

Although QC affects all modern digital systems, vehicles are more susceptible to the dangers of QC for several reasons:

1. Vehicles have a relatively long life cycle. New vehicles entering the market today will stay on the road for approximately 15 years, with the current average age of a passenger car in the US being around 12 years and rising[5][6]. Electric cars are expected to have even longer life spans[6][7].

[1] [1] The next tech revolution: quantum computing
[2] Quantum Cryptographic Threat Timeline

[2] [3] IBM Quantum

[3] [4] Kyber – Wikipedia

[4] [5] Falcon (signature scheme) – Wikipedia

[5] [6] Average Age of Automobiles and Trucks in Operation in the United States | Bureau of Transportation Statistics

[6] [7] EV Lifespan: Do They Last as Long as Gasoline Cars?

2. ECUs are typically harder to update than personal computers and mobile devices. This is especially true for their cryptographic capabilities, which are often implemented in a dedicated hardware component, called a Hardware Security Module (HSM) or Secure Hardware Extension (SHE), making it impossible to change the cryptographic schemes without a change of hardware. Some ECUs can be updated seamlessly over the air, but many can only be updated in registered service stations using dedicated tools.

3. Vehicles are composed of dozens of ECUs (sometimes more than 100), with the number of ECUs constantly rising in recent years[7][8]. In most cases, several different ECUs will have to be upgraded inside a single vehicle to ensure its safety.

This combination of old software and hardware, longer lifespans than laptops and smartphones as well as the complexity of updating multiple systems, creates a situation where vehicles that are vulnerable to QC-related attacks will likely remain on the streets for years.

## Fast forward to 2035: Future attack scenario

As a security researcher, I have learned the value of telling a story. Quite often, a vulnerability will remain unfixed because the developers aren't convinced that it could have real-world ramifications.

A compelling story can help a client understand the risk potential of a security issue. Equally important, telling yourself a story as a security researcher can guide you towards the more significant issues and research branches. The following future scenario illustrates the chain of events and the potential impact of a QC-enabled attack on a vehicle fleet.

> *It is the year 2035. "Gamamzone", the leading cloud services provider, has just launched its online Quantum Computing Services, falling a tad behind "Boogle", the search engine empire, that launched a similar platform just three months prior. For the low price of $1000 an hour, anyone can run their program on a fully functional remote quantum computer that is able to break any cryptographic scheme within a few hours.*
>
> *Bobby Malicious, an ill-tempered cyber-terrorist seeking to cause havoc, identifies the FOTA mechanism of old vehicles as a promising attack vector. He targets the 2025 AutoCar Plutonium, an older model that is vulnerable to post-quantum attacks but still has more than 100,000 instances on the road. He manages to gather the necessary funds and utilizes the quantum computer to easily bypass all cryptographic obstacles. Being a former employee of a major automotive cyber security firm, the attacker develops a malicious update and uploads it to all the 2025 Plutoniums with internet connectivity. The attacker now has complete control over tens of thousands of vehicles and is able to remotely immobilize them, or worse – cause them to slam the brakes in mid-drive. For his sinful achievements, Bobby is crowned king of cyber-terrorism, ushering in a bleak era in human history.*

While this story is still closer to sci-fi than tomorrow's news broadcast, many aspects of it might woefully prove to be very real in the not-too-distant future.

## Mitigating the quantum computing risk in the automotive landscape

Now that we've seen that the danger is real, let's discuss possible mitigation measures. The naive and more obvious approach to solve this problem would be to replace the cryptographic schemes in the automotive landscape with Post-Quantum Cryptographic (PQC) schemes, both in existing vehicles and those in development.

[7] [8] Number of automotive ECUs continues to rise

This approach will surely be adopted in the coming years when PQC will become the new standard (work related to PQC in the automotive landscape is already underway[8][9][10]). However, in the meantime, this solution might prove unfavorable for a number of reasons:

As previously mentioned, in many cases, it might be difficult or even impossible to update existing ECUs to have PQC capabilities.

1. HSMs are still not equipped with PQC capabilities (although some architectures have already been proposed[9][11]). Since vehicles heavily rely on HSMs for cryptography, it would be impossible for some ECUs to have PQC capabilities before HSMs have them.

2. PQC schemes are not as well attested as their pre-quantum counterparts, such as RSA and ECC. This means that it is somewhat more probable that the mathematical problems at the basis of the PQC schemes will turn out to be not as difficult as once thought, rendering them unsafe to use. The libraries implementing these schemes haven't been through the same constant review by cyber security experts, and are more likely to contain vulnerabilities and security issues. PQC schemes are currently under inspection by NIST, but this process is extremely elaborate and is not yet over[10][12].

Based on the above,  updating the cryptographic components of existing ECUs to PQC and designing new ones with only PQC capabilities is not yet feasible, and is not necessarily the smartest option.

Nevertheless, there are still a number of ways to reduce the security risks presented by QC, until the obvious approach becomes feasible. In the technical sphere, here are a few suggestions:

1. Doubling the key size in symmetric cryptographic schemes, such as AES (essentially increasing AES key length to 256 in alignment with NIST recommendations for key length[11][13]).

2. Complementing existing cryptographic schemes with PQC schemes, where possible. In such a scenario, both pre-quantum cryptographic schemes and PQC would have to be compromised for the mechanism to fail. This should be cautiously implemented to avoid a single point of failure.

3. In cases where adding PQC schemes is not possible, consider complementing asymmetric cryptographic schemes with symmetric schemes, such as HMAC for authentication.

From an administrative standpoint, awareness of QC risks is paramount for the automotive industry, and should be taken into account when designing a new ECU or vehicle architecture. This would allow vehicle manufacturers to keep QC-vulnerable ECUs away from safety-critical components, reducing the impact QC would have on the vehicle. In parallel, pressure should be put on HSM manufacturers to have automotive-oriented HSMs with PQC capabilities as soon as possible. Moreover, manufacturers should prepare update, upgrade and recall plans in advance to be ready for a potential QC-based attack.

## Final Thoughts

To recap, current development trends indicate that quantum computers might be coming sooner than

[8] [9] QuantumRISC
[10] RUB-Repository – Quantum safe authenticated key exchange protocol for automotive application

[9] [11] Post-Quantum Secure Architectures for Automotive Hardware Secure Modules

[10] [12] Post-Quantum Cryptography | CSRC

[11] [13] NIST.SP.800-57pt1r5.pdf

you think, and the security implications of this new computing paradigm must be considered.

Quantum Computing could significantly impact the automotive industry, as it is more susceptible than other industries to QC-related risks. Accordingly, automotive players should begin to think about the possible effects of Quantum Computing ASAP. New designs should incorporate encryption schemes, functionality, and recovery plans to cope with the arrival of fully functional and attainable quantum computers in the foreseeable future.

# 26.China's Latest Quantum Computer 'Wukong' To Debut, Production Line In Full Capacity

by CGTN
https://news.cgtn.com/news/2023-02-03/Production-line-for-China-s-latest-quantum-computer-in-full-capacity-1h7x6vJzuE0/index.html

China's first quantum chip production line made its debut via a live streaming program by China Media Group (CMG) on Tuesday, where Wukong, the country's latest quantum computer is to come out.

Quantum chips dedicated for Wukong had been developed at the production line by the end of last year, and are now debugging in the new quantum computer, said Jia Zhilong, deputy director of Anhui Quantum Computing Engineering Research Center, which is jointly established by Hefei Origin Quantum Computing Technology (Origin Quantum), a startup headquartered in Hefei, capital of east China's Anhui Province and Key Laboratory of Quantum Information of Chinese Academy of Sciences.

The country's latest quantum computer Wukong will feature a chip with over 64 qubits, Zhang Hui, manager of Origin Quantum, told guancha.cn in an interview, comparing to IBM's Osprey quantum processor with 433 qubits and Google's quantum chip Bristlecone with 72 qubits.

Zhang said the company lags behind the world's leading quantum computing players like IBM and Google in terms of hardware products and development, but has some advantages in the software and operating systems, and views the former as the way forward.

## Sharp 'eye' and ‘scalpel'

More cutting-edge tools have been developed to facilitate the production of quantum computers at the production line.

NDPT-100, China's first non-destructive probe electrical measurement platform, was developed by Origin Quantum in December, 2022.

Fast and accurate, the platform serves as a sharp eye to measure quantum bit resistance and can identify the quality of quantum chips with almost zero damage, greatly improving development efficiency.

The company built the country's first laser annealer in the following month. Dubbed "MLLAS-100," the laser annealer targets solving instability when the number of quantum bits increases.

It can achieve an ultra-high positioning accuracy of 100 nanometers and perform local laser annealing in a single quantum bit, enabling the quantum chip to expand to multiple bits.

Acting like a scalpel in surgery, it can accurately remove defects in quantum chips and improve production quality.

In the production process of quantum chips, the NDPT-100 platform is used to detect defective parts which will then be processed by the laser annealer, introduced by Jia. "With the pair cooperating with each other, quantum chips with higher quality are produced."

Based on an internal evaluation, "the yield of chips has been improved by about 10 times by utilizing these two machines," Jia told CMG.

Since its operation in January 2022, the production line has introduced 24 sets of quantum chip production equipment, incubated three sets of special equipment for quantum chips, and delivered multiple batches of quantum chips and quantum amplifiers, said Jia.

# 27.China Unveils Massive Blockchain Cluster Running Homebrew Tech

**by Simon Sharwood**
https://www.theregister.com/2023/02/03/china_1000_server_blockchain_cluster/

China's ambition to record government and commercial activity on a blockchain has a new engine: a 1,000-server cluster in Beijing capable of handling 240 million smart contract transactions each second.

The machine is notable for two reasons.

One is that this rig uses homegrown tech. The cluster is linked to ChainMaker – a made-in-China blockchain platform that's been contributed to and/or adopted by significant Chinese private and government enterprises. ChainMmaker has also claimed to have developed 96-core silicon designed to accelerate blockchain transactions. The Beijing Academy of Blockchain and Edge Computing – understood to be the designer of the facility – has previously announced it has developed petabyte-scale storage systems.

With the USA leading bans on export of high tech to China, rigs like this show that Beijing can build big and complex things.

The second reason is that this rig demonstrates that Beijing's drive for extensive blockchain use is real, and ready to roll.

As state-controlled media reports on the cluster explain, it will be used to secure and record transactions across 80 departments, 16 districts, and organizations in the fields of transportation, finance, and telecommunications, and is intended to ensure information flows back to Beijing to realize "efficient coordination of the governance system."

And at quite a scale, suggesting China is going to make smart contracts an important part of its business environment.

It's just the sort of thing one might expect in a single party state that exercises close control over economic development and likes to keep tabs on organizations' performance.

The rig is likely one of Earth's mightiest blockchain implementations, which will give boosters of such technology heart. Expect them to promote its use – and distinguish those efforts from the wretched hive of scum and villainy that infected the cryptocurrency scene.

# 28.Developers, It's Time To Prepare For The Quantum World!

by LV Subramaniam
https://www.dqindia.com/developers-its-time-to-prepare-for-the-quantum-world/

Over the last few years, quantum computing has emerged as an exciting new technology that promises to shape our world of tomorrow through a myriad of possibilities. Advances in quantum computing could open the door to new scientific discoveries, life-saving drugs, and drastic improvements in supply chains, logistics and the modelling of financial data.

While the technology is still evolving, it is widely expected to bring a paradigm shift in computing, by far exceeding the capabilities of today's most powerful classical supercomputers. Not surprisingly, the market for quantum computing is expected to grow to USD18.16 billion by 2030 according to a Market Research Future report.

## Opportunity for Developers

The Government of India announced the National Mission on Quantum Technologies and Applications (NMQTA) acknowledging that quantum computing has the potential to bring about a major technological disruption in the world of computing, communication, security, and touch every industry. At the core of this mission is building skilled manpower.

According to a NASSCOM and Avasant Report on the Quantum Revolution, NMQTA aims to develop a quantum skilled workforce of about 25,000- 30,000 resources across software, hardware, and allied tech. For the quantum industry to take off in India, it will require both quantum-aware and quantum-proficient engineers, scientists, and managers.

Innovations in quantum computing are compelling industry leaders around the globe to mobilize workforces and harness the disruptive possibilities of the quantum world. There is a growing demand for the right software skills to program the hardware and develop these quantum applications.

For developers, there couldn't be a better time to build quantum coding skillsets that will make them highly coveted by prospective employers. With so much potential for research in this exciting new world, a spirit of inquiry and curiosity is a de facto requirement for developers.

## Building career path in quantum computing

While the opportunities are endless, the question is: how can a professional make inroads into the field of quantum computing? Irrespective of their current field of specialization, quantum computing will require a certain degree of learning, unlearning, and relearning. Here are a few steps to consider:

- **Evaluate the opportunities**

  There are several kinds of roles at play for quantum computing. These could be roles in hardware or systems, which require knowledge of physics and engineering. There are opportunities for Kernel developers with skills in engineering, physics, and programming, algorithm developers with a background in computer science or physics, application developers with domain knowledge as well as programming skills in languages such as Python. Identifying the role that is right for you is the first step before you build the right profile and gain certification/training.

- **The right training**

  In addition to strong fundamentals in programming, a career in quantum computing requires skills in analytical reasoning, a collaborative mindset, and domain knowledge. Familiarity with optimizers in AI/ML/DL can help developers make quantum algorithms more effective.

  The ability to develop, test, deploy software built on open-source platforms is an advantage while building quantum software development kits (Qiskit). Investment in building these skills whether through enrolling in online or physical classes with a reputed institute or taking free online courses can provide a good head start.

  While there are several Universities that offer masters programs and also part time PhDs (industry sponsored research is also an opportunity) for others, they can also opt for Developer certifications programs that validate their knowledge, expertise and skills.

- **Hands-on experience**

  Getting hands on access to actual quantum computers and running programs on it can prove to be valuable. Today, several quantum software development kits are open source — easily accessible to anyone over the cloud. There are also over 300+ courses available online with learning modules and access to quantum systems for anyone looking to get a hands on experience in programming quantum circuits and running them.

  For instance, Qiskit allows anyone to program real quantum computing hardware, requiring only Python and a basic knowledge of linear algebra as a prerequisite. Since IBM launched Qiskit in 2017, thousands of users have developed applications, maintained and improved code, and taken part in both live and virtual hackathons, summer schools, and other educational opportunities to build this vibrant, open-source community. We think, we can aim our sights even higher!

The quantum age promises tremendous game-changing possibilities across disciplines such as chemistry, machine learning, finance, logistics, and physics to solve deeper programs.

R&D efforts are gaining momentum as more countries and corporations enter the race for advantage in the quantum world. If we want to make the world quantum safe, there is an opportunity to use emerging quantum safe standards for better cyber security.

With India’s advantageous position as a global hub for digital talent, developers have an opportunity to build the right skills and surge ahead in the field of quantum computing.

# 29.U.S., India Hold First Meeting To Coop-

# erate On Building Quantum, Deep Tech Ecosystem

by Matt Swayne
https://thequantuminsider.com/2023/02/02/u-s-india-hold-first-meeting-to-cooperate-on-building-quantum-deep-tech-ecosystem/

A team of Indian and American officials held the first meeting of an organization developed to elevate and expand strategic technology partnership and defense industrial cooperation between the countries' governments, businesses and academic institutions. Quantum is one of the technological areas identified for cooperation.

Two National Security Advisors led the U.S.-India initiative on Critical and Emerging Technology's — or iCET — inaugural meeting, according to a White House statement. On the U.S. side, officials represented the Administrator of the National Aeronautics and Space Administration, the Director of the National Science Foundation, the Executive Secretary of the National Space Council, and senior officials from the Department of State, Department of Commerce, the Department of Defense, and the National Security Council. On the Indian side, the Ambassador of India to the United States, the Principal Scientific Advisor to the Government of India, the Chairman of the Indian Space Research Organization, the Secretary of the Department of Telecommunications, the Scientific Advisor to the Defense Minister, the Director General of the Defence Research and Development Organization, and senior officials from the Ministry of Electronics and Information Technology and the National Security Council Secretariat participated.

According to the statement: "The two sides discussed opportunities for greater cooperation in critical and emerging technologies, co-development and coproduction, and ways to deepen connectivity across our innovation ecosystems. They noted the value of establishing "innovation bridges" in key sectors, including through expos, hackathons, and pitch sessions. They also identified the fields of biotechnology, advanced materials, and rare earth processing technology as areas for future cooperation."

The partnership looked at ways of strengthening the Indian-American ecosystem for innovation, including plans to bolster high-performance computing, artificial intelligence and quantum technological research and development. The bilateral initiatives include:

- Signing a new Implementation Arrangement for a Research Agency Partnership between the National Science Foundation and Indian science agencies to expand international collaboration in a range of areas — including artificial intelligence, quantum technologies, and advanced wireless — to build a robust innovation ecosystem between our countries.

- Establishing a joint Indo-U.S. Quantum Coordination Mechanism with participation from industry, academia, and government to facilitate research and industry collaboration.

- Drawing from global efforts to develop common standards and benchmarks for trustworthy AI through coordinating on the development of consensus, multi-stakeholder standards, ensuring that these standards and benchmarks are aligned with democratic values.

- Promoting collaboration on High Performance Computing (HPC), including by working with Congress to lower barriers to U.S. exports to India of HPC technology and source code.

# 30.IoT Authentication Platform Adds Quantum-Hardened Private Keys

by Jean-Pierre Joosting
https://www.eenewseurope.com/en/iot-authentication-platform-adds-quantum-hardened-private-keys/

Quantinuum, a leading integrated quantum computing company, has announced that Cybertrust Japan Co., Ltd., Japan's leading certificate authority, has integrated its Quantum Origin quantum-computing-hardened private keys into a new certificate issuance and distribution platform for IoT devices to ensure secure communications now and into the future.

Cybertrust Japan's new authentication infrastructure for high-speed, high-volume certificate issuance and distribution for large volumes of IoT devices includes the NIST-selected post-quantum cryptography (PQC) algorithms. The certificate authority is further protecting devices from current and advancing threats by incorporating Quantum Origin, the only cryptographic offering that leverages the power of quantum computers to generate quantum-computing-hardened keys.

"Integrating Quantum Origin assures our customers that they can build innovative IoT-based solutions on a platform they can trust to deliver speed and higher security, including post-quantum algorithms support. As a result, customers and partners can use and sell our certification services securely for the long term," said Yasutoshi Magara, President and CEO of Cybertrust Japan.

IoT devices typically use certificates to authenticate their connection to other devices or networks to prove that they are trusted devices. The challenge when providing and managing certificates across these devices is complex because of the volume of devices trying to connect to networks and the need to provide fast access to data. Security measures need to be robust while also enabling real-time communications.

"Cybertrust Japan and Quantinuum have shown that an advanced quantum-computing-based solution like Quantum Origin can be seamlessly integrated into authentication infrastructure to strengthen key and certificate generation. Cybertrust Japan is the first certification provider in the world to support quantum-computing-hardened keys using Quantum Origin," said Duncan Jones, Head of Cybersecurity at Quantinuum. "As the use of IoT devices grows, companies must ensure that their devices have state-of-the-art protection against increasingly sophisticated cyberattacks that threaten their most valuable assets and data. Quantum Origin is the only offering that provides encryption keys generated by quantum computers giving customers an unrivalled ability to strengthen existing security measures and reduce their risk of exposure from advanced encryption-based attacks."

Cybertrust Japan's Secure IoT Platform protects end devices through the entire product lifecycle from semiconductor design to the implementation of the devices to the ultimate disposal of the devices. The Secure IoT Platform creates security certificates for the manufacturing process to protect the hardware, to make the manufacturing process traceable and to provide a long-term defect warranty. The product also includes a management platform for the devices to allow secure OS and software updates in addition to securing the data created and transmitted by the devices.