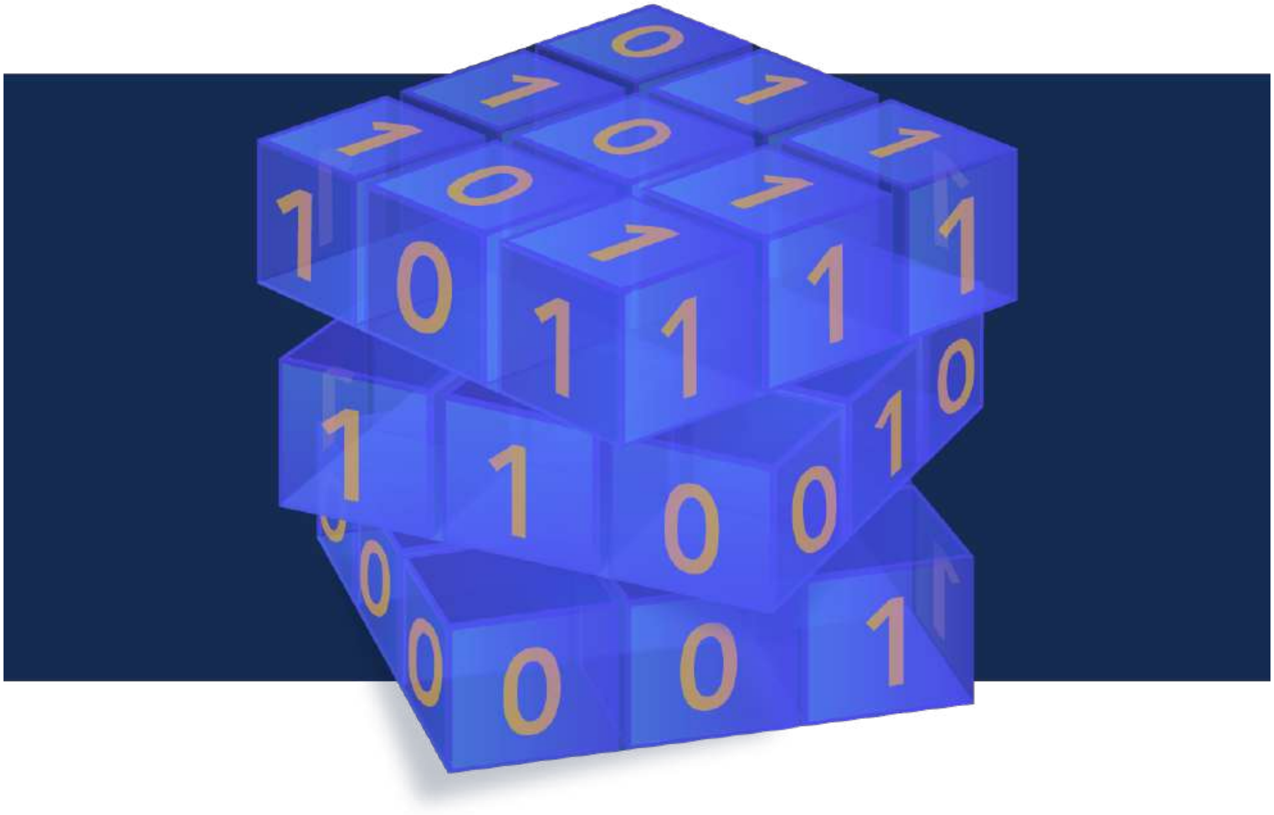
Crypto News

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

October 01, 2022



TABLES OF CONTENTS

Editorial

It's time for fall but also "spooky season" with Halloween right around the corner. Whether you celebrate Halloween or not, there's plenty of scary stuff out there these days that keeps us technology professionals up at night. Fear not though! The best cure for that anxious mind is knowledge. Read this month's issue of Crypto News to get some well-deserved rest!

Let's start with article 17 which speaks to the National Security Agency (NSA) in the United States goal to implement pos-quantum algorithms by 2035. Will that be fast enough though? According to article 27 (and the CSA QSS working groups own countdown clock found here), the answer is a resounding no. There are a number of countries who participate in the world scientific community and share their work and progress in regards to quantum computing, however, there are other nation states that do not. It is these nation states that are the reason for the prediction that 2030 is more than likely when we will face "Y2Q" (Year to Quantum) as noted by our own working group, the CSA Quantum Safe Security working group, as well as the author of this article. Bottom line, we all need to work faster to prepare and implement effective solutions for a post-quantum world.

Interestingly, an increasing number of cybersecurity professionals agree that quantum computing is already putting data at risk. They readily disclose that their organizations are susceptible to "harvest now, decrypt later" attacks. This is when cyber criminals will hack systems and extract encrypted data knowing that in time quantum computers will be able to break the current cryptographic algorithms. Want to learn more about what cybersecurity professionals are saying about quantum computers? Scroll to article 6. This issue is full of a number of other interesting article that you won't want to miss. See you next month!

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

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

1. GSMA, IBM and Vodafone Establish Post-Quantum Telco Network Taskforce

https://newsroom.ibm.com/2022-09-29-GSMA,-IBM-and-Vodafone-Establish-Post-Quantum-Telco-Network-Taskforce

The GSMA today announced the formation of the GSMA Post-Quantum Telco Network Taskforce, with IBM and Vodafone as initial members, to help define policy, regulation and operator business processes for the enhanced protection of telecommunications in a future of advanced quantum computing.

Unlike today's computers that rely on bits for calculation, quantum computers harness the exponential power of quantum bits (qubits). This can be a complicated, simultaneous mix of 1s and 0s, creating the potential to solve extremely complex problems that challenge even the most powerful supercomputers today.

The GSMA Post-Quantum Telco Network Taskforce will help define requirements, identify dependencies and create the roadmap to implement quantum-safe networking, mitigating the risks associated with future, more-powerful quantum computers. Without quantum-safe controls in place, sensitive information such as confidential business information and consumer data could be at risk from attackers who harvest present-day data for later decryption. The World Economic Forum recently estimated that more than 20 billion digital devices will need to be either upgraded or replaced in the next 10-20 years to use the new forms of quantum-safe encrypted communication.

"The GSMA Taskforce's goal is to bring together leading global communication services providers with experts from IBM, Vodafone and other operators and ecosystem partners to understand and implement quantum-safe technology. By working together to establish consistent policies, we can define quantum-safe approaches that protect critical infrastructure and customer data, complementing our ongoing security efforts to increase resiliency in future networks," said Alex Sinclair, the GSMA's Chief Technology Officer.

To address the challenges presented by emerging quantum technology, the U.S. National Institute of Standards and Technology (NIST) announced in July 2022 that it had chosen the first four post-quantum cryptography algorithms to be standardised for cybersecurity in the quantum computing era. These algorithms are designed to rely on the computational difficulty of problems from the mathematical areas of lattices, isogenies, hash functions and multivariate equations — and protect today's systems and data from future quantum computers.

IBM, a leader in cryptography and pioneer in quantum technology – with the world's largest fleet of cloud-accessible quantum computers – contributed to the development of three of NIST's four chosen post-quantum algorithms.

“Given the accelerated advancements of quantum computing, data and systems secured with today’s encryption could become insecure in a matter of years. IBM is pleased to work with the GSMA Post-Quantum Telco Network Taskforce members to prioritize the telco industry’s move to adopt quantum-safe technology,” said Scott Crowder, Vice President of IBM Quantum Adoption and Business Development.

“In a modern Hybrid Cloud world, communications services and compute technologies are interconnected and underpin all industries, which means the adoption of quantum-safe cryptography in telecom will affect all enterprises and consumers. This taskforce will support the telco industry by creating a roadmap to secure networks, devices and systems across the entire supply chain,” said Steve Canepa, General Manager, Global Industries, IBM.

Luke Ibbetson, Head of R&D, Vodafone, said: “Quantum computing is by far the biggest revolution in computing since the 1950s, and most of it will have a positive impact on our industry and society as we move towards fully automated networks. It has the potential to solve highly complex optimisation challenges which may allow us to further fine-tune our networks for an even better customer experience.

“At the same time, future quantum computing could inherently undermine the cryptographic principles relied on today. That is why Vodafone is committed to working with the GSMA and other members of the GSMA Post-Quantum Telco Network Taskforce to protect and secure customer data with the timely adoption of quantum-safe solutions, policies and standards.”

The GSMA Post-Quantum Telco Network Taskforce will convene to drive consensus and adoption in this new field and it will be oriented across three areas:

- **Strategy** – to integrate quantum-safe capabilities into telco network operators’ technology, business processes and security.
- **Standardisation** – to identify the needs and common alignments for the integration of quantum-safe capabilities into existing telco networks.
- **Policy** – to advise on telco network public policy, regulation and compliance and to ensure scale across the industry.

2. NATO Using Quantum Technologies to Make Communications Secure

by James Dargan
https://thequantuminsider.com/2022/09/29/nato-using-quantum-technologies-to-make-communications-secure/?utm_source=newsletter&utm_medium=email&utm_term=2022-10-01&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Rockin+The+Rockies+OQC+Cloud+Collab+And+More+Quantum+News

Innovative projects led by scientists in NATO and partner countries are breaking new ground to harness the power of quantum to make communications impossible to intercept and hack. The application of these quantum technologies in the security and defence sectors could help to future-proof the transmission of information, protecting it from increasingly advanced hacking systems and contributing to NATO's efforts to maintain its technological edge.

NATO Science for Peace and Security (SPS) Programme research and development projects have been examining the security-related applications of quantum technologies, addressing their three main fields: computing, sensing and communications. Quantum computing and sensing are improving the abilities of computer and remote measurement technologies to levels that they are not traditionally able to achieve. In the field of quantum communications, SPS activities are showing the most promising results. These projects develop systems for the encryption and secure transmission of information using quantum key distribution (QKD) and post-quantum cryptography (PQC). Through these techniques, they respond to rising security concerns related to new technologies—such as quantum computers, which can decipher secret communications—by preventing unauthorised access.

Testing quantum key distribution (QKD)

QKD is a quantum communication method to share decryption keys. In this system, an encrypted message is sent over traditional networks, while the keys to decrypt the information are transmitted through quantum means. This way, only the intended recipient can decode the message, making any eavesdropping impossible. By applying this method, an SPS project succeeded in connecting Italy and Malta with a prototypical QKD link using submarine optical fibre cables for the first time.

Another SPS-supported research initiative investigated QKD techniques to send cryptographic keys from one endpoint to another, which was located hundreds of kilometres away. Meanwhile, researchers at a university in the Czech Republic are studying the application of QKD technology on a 5G network to explore its potential to enhance cyber security in future communication systems.

Demonstrating post-quantum cryptography (PQC)

Unlike QKD, which uses physical quantum properties to protect information, PQC uses cryptography and mathematical functions as an alternative approach to secure communications. An international group of scientists supported by SPS recently demonstrated that, using PQC, it is possible to securely transmit information without the possibility of decryption by a hacker, even one who has a quantum computer. Through a secure protocol, five research groups based in Malta, Slovakia, Spain, the United States and NATO Headquarters in Brussels, Belgium, succeeded in communicating in a completely secure space, free from the risk of intrusion.

NATO's new Strategic Concept, agreed by Allies at the 2022 Madrid Summit, recognises the critical role of technology, and in particular, emerging and disruptive technologies (EDTs), in shaping the future of the Alliance. To explore the potential and risks associated with EDTs, the SPS Programme is supporting research activities that address technological trends in EDTs, like artificial intelligence, autonomy, bioengineering, and especially quantum technologies. Future SPS activities investigating quantum will look at how to integrate both QKD and PQC to secure information infrastructure in the best and most holistic way for the Alliance.

3. Traditional computers can solve some quantum problems

by California Institute of Technology
https://www.sciencedaily.com/releases/2022/09/220923090705.htm

A new study describes how machine learning tools, run on classical computers, can be used to make predictions about quantum systems and thus help researchers solve some of the trickiest physics and chemistry problems.

There has been a lot of buzz about quantum computers and for good reason. The futuristic computers are designed to mimic what happens in nature at microscopic scales, which means they have the power to better understand the quantum realm and speed up the discovery of new materials, including pharmaceuticals, environmentally friendly chemicals, and more. However, experts say viable quantum computers are still a decade away or more. What are researchers to do in the meantime?

A new Caltech-led study in the journal Science describes how machine learning tools, run on classical computers, can be used to make predictions about quantum systems and thus help researchers solve some of the trickiest physics and chemistry problems. While this notion has been shown experimentally before, the new report is the first to mathematically prove that the method works.

"Quantum computers are ideal for many types of physics and materials science problems," says lead author Hsin-Yuan (Robert) Huang, a graduate student working with John Preskill, the Richard P. Feynman Professor of Theoretical Physics and the Allen V. C. Davis and Lenabelle Davis Leadership Chair of the Institute for Quantum Science and Technology (IQIM). "But we aren't quite there yet and have been surprised to learn that classical machine learning methods can be used in the meantime. Ultimately, this paper is about showing what humans can learn about the physical world."

At microscopic levels, the physical world becomes an incredibly complex place ruled by the laws of quantum physics. In this realm, particles can exist in a superposition of states, or in two states at once. And a superposition of states can lead to entanglement, a phenomenon in which particles are linked, or correlated, without even being in contact with each other. These strange states and connections, which are widespread within natural and human-made materials, are very hard to describe mathematically.

"Predicting the low-energy state of a material is very hard," says Huang. "There are huge numbers of atoms, and they are superimposed and entangled. You can't write down an equation to describe it all."

The new study is the first mathematical demonstration that classical machine learning can be used to bridge the gap between us and the quantum world. Machine learning is a type of computer application that mimics the human brain to learn from data.

"We are classical beings living in a quantum world," says Preskill. "Our brains and our computers are classical, and this limits our ability to interact with and understand the quantum reality."

While previous studies have shown that machine learning applications have the ability to solve some quantum problems, these methods typically operate in ways that make it difficult for researchers to learn how the machines arrived at their solutions.

"Normally, when it comes to machine learning, you don't know how the machine solved the problem. It's a black box," says Huang. "But now we've essentially figured out what's happening in the box through our numerical simulations." Huang and his colleagues did extensive numerical simulations in collaboration with the AWS Center for Quantum Computing at Caltech, which corroborated their theoretical results.

The new study will help scientists better understand and classify complex and exotic phases of quantum matter.

"The worry was that people creating new quantum states in the lab might not be able to understand them," Preskill explains. "But now we can obtain reasonable classical data to explain what's going on. The classical machines don't just give us an answer like an oracle but guide us toward a deeper understanding."]Co-author Victor V. Albert, a NIST (National Institute of Standards and Technology) physicist and former DuBridge Prize Postdoctoral Scholar at Caltech, agrees. "The part that excites me most about this work is that we are now closer to a tool that helps you understand the underlying phase of a quantum state without requiring you to know very much about that state in advance."

Ultimately, of course, future quantum-based machine learning tools will outperform classical methods, the scientists say. In a related study appearing June 10, 2022, in Science, Huang, Preskill, and their collaborators report using Google's Sycamore processor, a rudimentary quantum computer, to demonstrate that quantum machine learning is superior to classical approaches.

"We are still at the very beginning of this field," says Huang. "But we do know that quantum machine learning will eventually be the most efficient."

4. Peter Shor wins Breakthrough Prize in Fundamental Physics

by Jennifer Chu
https://news.mit.edu/2022/shor-spielman-breakthrough-prize-0922

Peter Shor, the Morss Professor of Applied Mathematics at MIT, has been named a recipient of the 2023 Breakthrough Prize in Fundamental Physics. He shares the $3 million prize with three others for "foundational work in the field of quantum information": David Deutsch at the University of Oxford, Charles Bennett at IBM Research, and Gilles Brassard of the University of Montreal.

In announcing the award, the Breakthrough Prize Foundation highlighted Shor's contributions to the quantum information field, including the eponymous Shor's algorithm for factoring extremely large numbers, and for an algorithm to correct errors in quantum computers.

"These ideas not only paved the way for today's fast-developing quantum computers; they are now also at the frontiers of fundamental physics, especially in the study of metrology — the science of measurement — and of quantum gravity," the award announcement reads.

"I'm very grateful to see the prize going to quantum information and quantum computation theory this year," Shor commented to MIT News. "My three co-winners were the most influential people in founding this field. I consider them friends, and they all clearly deserve it."

In addition, an MIT alumnus, Daniel A. Spielman PhD '95, has won the 2023 Breakthrough Prize in Mathematics for "contributions to theoretical computer science and mathematics, including to spectral graph theory, the Kadison-Singer problem, numerical linear algebra, optimization, and coding theory."

"I am ecstatic to see both Peter Shor and Dan Spielman be recognized with Breakthrough Prizes in Fundamental Physics and Mathematics, respectively," says Michel Goemans, the RSA Professor and head of MIT's Department of Mathematics. "Both would have been natural nominees of the Breakthrough Prize in Theoretical Computer Science, if such a prize existed. Peter and Dan are PhD graduates of our math department, both have held tenured appointments in our department and have been members of the theory group at CSAIL, and both have received the same prizes. It is a testimony of the importance of theoretical computer science across disciplines, in particular mathematics and physics."

Quantum seeds

The first seeds of quantum computing's potential were planted through the early algorithms derived by Deutsch, Bennett, Brassard, and Shor.

In the early 1980s, Deutsch began thinking of problems whose solutions could be sped up using quantum algorithms — formulas that were derived using the laws of quantum mechanics, rather than classical physics. He was the first to develop a quantum algorithm that could solve a simple, albeit contrived, problem far more efficiently than a classical algorithm.

Meanwhile, Bennett and Brassard were also looking for uses of quantum information. In 1984, they developed the first quantum cryptography protocol, BB84. They put forth the idea that two distant parties could agree on a secret encryption key, which would be secure against eavesdroppers, based on a strange quantum principle in which the value of the encryption key would instantly be disturbed and therefore unreadable when measured.

Their work demonstrated the first practical application of quantum information theory. It was also Shor's first introduction to the field. The mathematician was working at AT&T Bell Labs at the time, and Bennett came to give a talk on his new quantum key encryption system. "Their work inspired me to do a little thinking and research on quantum information," Shor recalls. "But I didn't really get anywhere at the time."

A decade later, in 1994, Shor introduced his own landmark algorithm. Shor's algorithm describes how a sufficiently large quantum computer could efficiently factorize extremely large numbers — a task that would take more than the age of the universe for the most powerful classical supercomputer to solve.

Most data encryption schemes today rely on the difficulty of factorization to keep information secure. Shor's algorithm was the first to show that, in theory, a quantum system could break through most modern data security walls. To do this practically, however, would require a system of many precisely controlled quantum bits. Even then, scientists assumed that the tiniest noise in the environment would disrupt the delicate qubits, and set off a ripple of errors in their calculations that could not be corrected without further disturbing the qubits.

"When I first came up with this factoring algorithm, people thought it would remain theoretical forever because there was this argument that you could not correct errors on a quantum computer," Shor says.

Shortly thereafter, in 1995, Shor worked out another algorithm, this time on quantum error correction, which showed that errors in a quantum system could in fact be isolated and fixed without disturbing the qubit itself, thereby leaving the quantum computation intact. The vision of a practical quantum computer became immediately tangible.

"With these two bombshell contributions, Peter set the stage for quantum computing to become the huge field that it is now," says Alan Guth, the Victor F. Weisskopf Professor of Physics at MIT, who as a former recipient of the Breakthrough Prize, was the one who called Shor to deliver the news of this year's award.

"It was a real pleasure for me to be able to tell him that he is one of the winners," Guth says. "His algorithms took the world by surprise, and ignited the field of quantum computing. And despite his spectacular contributions, Peter continues to be a warm, friendly, smiling colleague to all around him."

"Peter is a wonderful colleague and is totally unique," adds Goemans. "His thought process seems to parallel the quantum algorithms he designs and invents: Out of entangled ideas and a superposition of states, a brilliant solution often emerges in a Eureka moment!"

"One of the best things about MIT is that we have great students," says Shor, who earned a PhD in applied mathematics from MIT in 1985. He then spent one year as a postdoc at the Mathematical Sciences Research Institute before moving on to work at AT&T Bell Labs, where he developed Shor's algorithm. In 2003, he returned to MIT, where he has continued his research and teaching for the past 20 years.

Today, he is working to formulate a theory of quantum information, which would describe how data can be stored and transmitted, using the principles of quantum physics. Will there come a day when quantum computers are advanced enough to break through our classical security systems?

"In five or 10 years, we could be at the start of a Moore's Law, where quantum computers will steadily improve every few years," Shor predicts. "I suspect they'll improve fast enough that within two or three decades we will get quantum computers that can do useful stuff. Hopefully by the time quantum computers are that large, we'll be using different crypto systems that aren't susceptible to quantum computers."

Shor credits his father with fostering his early interest in mathematics. As a young boy, would flip through his father's issues of Scientific American, to find his favorite section.

"Martin Gardner had a column, 'Mathematical Games,' which was really amazing," Shor recalls. "It was sometimes a puzzle, sometimes a report on a new discovery in mathematics, and it was often at a level that I could understand. I looked forward to reading it every month, and that was something that turned me onto math early on."

Beautiful breakthroughs

Daniel Spielman, this year's recipient of the Breakthrough Prize in Mathematics, received a PhD in applied mathematics at MIT in 1995, for which he was advised by Michael Sipser, the Donner Professor of Mathematics and former dean of the MIT School of Science. Spielman then joined the math department and was on the MIT faculty until 2005, before moving on to Yale University, where he is currently the Sterling Professor of Computer Science, Mathematics, Statistics and Data Science.

Spielman specializes in the design and analysis of algorithms, many of which have yielded insights "not only for mathematics, but for highly practical problems in computing, signal processing, engineering, and even the design of clinical trials," notes the Breakthrough Foundation in their announcement today.

"Dan has made a number of important and beautiful breakthroughs over the years, from expander-based error-correcting codes, to the smoothed analysis of algorithms, or spectral sparsifications of graphs, all characterized by innovative mathematics," says Goemans.

Among numerous discoveries, Spielman is best known for solving the Kadison-Singer problem, which for decades was thought to be unsolvable. The problem can be interpreted as posing a fundamental question for quantum physics: In a quantum system, can new information be deciphered, if only some of the system's properties are observed or measured? The answer, most mathematicians agreed, was no.

Over decades, the Kadison-Singer problem was reformulated and shown to be equivalent to problems across a wide range of mathematical fields. And in 2013, Spielman and his colleagues resolved one of these equivalent formulations involving linear algebra and matrices, proving the answer to be yes — indeed, it was possible to determine a quantum system's sum from its parts.

The Breakthrough Prizes are a set of international awards that recognize the achievements of scientists in three categories — fundamental physics, mathematics, and life sciences. The prizes were founded by Sergey Brin; Priscilla Chan and Mark Zuckerberg; Julia and Yuri Milner; and Anne Wojcicki, and have been sponsored by foundations established by them. The 2023 prizes will be presented at a gala award ceremony, and prize recipients will take part in lectures and discussions.

5. Brown mathematicians' algorithm to serve as cryptography standard for quantum computing era

by Mary Stuart
https://www.brown.edu/news/2022-09-21/cryptography

The federal government selected four algorithms to serve as standards for public key security in the pending era of quantum computers, three of which are based on technology devised by a team of Brown experts.

Mathematicians often toil in obscurity, and that's likely because few people, apart from fellow mathematicians who share the same sub-specialty, understand what they do. Even when algorithms have practical applications, like helping drivers see approaching cars that the eye can't discern, it's the car manufacturer (or its software developer) that gets the credit.

This is especially true of cryptographers, the unsung heroes whose algorithms keep people's communications and data secure when they use the internet — technology known as public key cryptography.

But sometimes, pure math impacts the real world. That happened this summer when the National Institute of Standards and Technologies selected four cryptography algorithms to serve as standards for public key security in the impending era of quantum computers, which will make current encryption systems quickly obsolete.

Three of the four chosen algorithms rest on work led by a team of mathematicians at Brown: professors Jeffrey Hoffstein, Joseph Silverman and Jill Pipher (who also serves as Brown's vice president for research).

The story of the NIST-endorsed Falcon algorithm — and NTRU, the public key cryptosystem upon which Falcon is based — began in the mid-90s, when quantum computing was still in the realm of science fiction. At the time, Hoffstein's goal was to develop an algorithm to simplify and speed up the way conventional cryptographic algorithms worked; in 1996, he co-founded NTRU Cryptosystems Inc. with Silverman and Pipher (who is also married to Hoffstein) to take it to market. Hoffstein said the history of NTRU is a "bloodcurdling saga," but the company was ultimately successful, finding a suitable purchaser in Qualcomm. Falcon, which Hoffstein co-designed with nine other cryptographers, and two out of the three other algorithms NIST selected, are built upon the original NTRU framework.

From before his doctoral study at MIT through each of the positions he's held at the Institute for Advanced Study, Cambridge University, the University of Rochester and Brown, Hoffstein has been "a numbers guy," through and through: "It never occurred to me not to be a mathematician," he said. "I promised myself that I would continue to do math until it was no longer fun. Unfortunately, it's still fun!"

On the heels of NIST's selection, Hoffstein described his transformation from a number theorist to an applied mathematician with a solution to an impending global problem of critical importance.

Q: What is public key cryptography?

When you connect to Amazon to make a purchase, how do you know that you are really connected to Amazon, and not a fake website set up to look exactly like Amazon? Then, when you send your credit card information, how do you send it without fear of it being intercepted and stolen? The first question is solved by what is known as a digital signature; the second is solved by public key encryption. Of the NIST's standardized algorithms, one is for public key encryption, and the other three, including Falcon, are for digital signatures.

At the root of these are problems of pure mathematics of a very special type. They are hard to solve (think: time until the universe ends) if you have one piece of information and they are easy to solve (takes microseconds) if you have an extra piece of secret information. The wonderful thing is that only one of the parties communicating — Amazon, in this case — needs to have the secret piece of information.

Q: What is the security challenge that quantum computers pose?

Without a sufficiently strong quantum computer, the time to solve the encryption problem is eons. With a strong quantum computer, the time to solve the problem comes down to hours or less. To put it more alarmingly, if anyone had possession of a strong quantum computer, the entire security of the internet would completely break down. And the National Security Agency and major corporations are betting that within five years there is a good chance that a quantum computer strong enough to break the internet could be built.

Q: You came up with the NTRU solution in the early to mid-90s, well in advance of anyone thinking about the cryptography needs of potential quantum computers. What was your thinking at the time?

I found the three main approaches to public key cryptography to be very clunky and unaesthetic. Just as one example, the most well-known method, RSA, involves taking numbers that are many hundreds of digits long, then raising them to powers that are hundreds of digits long, dividing by yet another number that is hundreds of digits long, and finally taking the remainder. This computation is easily doable on a computer but not very practical if you have a small, lightweight processor, like a cell phone from 1996. RSA is also very slow — okay, milliseconds, but that still counts as slow.

Our dream was to find a method for doing public key cryptography that was orders of magnitude faster than RSA and could run on low-powered devices And we did it! People implementing it were able to run it at speeds 200 to 300 times faster than RSA. I didn't do this alone — I thought obsessively about the problem for a year and a half, but it didn't coalesce into a solution until I joined with Joe Silverman and Jill Pipher, my Brown colleagues and the co-founders of NTRU.

Q: What does NTRU stand for?

We never said — people just assumed we meant something technical and used their imaginations! But it stands for "Number Theorists R Us." This irritated Jill as she is a harmonic analyst, not a number theorist, but she eventually forgave me.

Q: You've described your start-up NTRU Cryptosystems as having about five "near death" experiences. What were some of the challenges you faced?

The gatekeepers in the field are mostly cryptographers who work for companies and in computer science departments. It is incredibly hard to get any new algorithm to be taken seriously, and it's particularly hard if you're not in the cryptography club. In our case, we rang alarm bells for two reasons. We were outsiders, for one, and we added extra structure from algebraic number theory to lattices to make things more efficient.

Whenever you do that, there is a serious risk that you have accidentally introduced weaknesses. Yes, it is wonderful to do something more efficiently. But have you lost some vital piece of security in the process? It is completely understandable that people were deeply suspicious of this extra structure, which introduced the ability to multiply as well as add. It took 10 years of intense scrutiny before people started to accept that no weaknesses had been added.

Q: This wasn't just an academic exercise. NTRU was a company that had to work with investors and potential customers. Early on, NTRU came unjustly under attack in a paper written by some household names in cryptography (who later acknowledged their error). How did NTRU survive that?

It turned out that their paper was largely ignored, but our paper was sufficiently interesting that everybody dove into it. They tried to attack and destroy it, and it got a tremendous amount of attention. Every single surface you can imagine was beset by battering rams. The cryptography community was so resistant to mathematicians encroaching on their turf. If we hadn't been well-known mathematicians from Brown, we wouldn't have survived the controversy. In the end, that attention probably helped us.

Q: Were there any ways in which being mathematicians — outsiders, this world — was an advantage?

The thing that I'm proudest of isn't necessarily the fact that the particular algorithm ended up in the final four of the NIST picks, although every single one of the three lattice-based algorithms uses our ring structure (the multiplication feature). They all use the math that we introduced because after more than 25 years of scrutiny, not a single weakness has come up because of adding that structure. That math, which came from algebraic number theory, wasn't part of cryptography before. It is part of what I do for my other living, and I find it particularly delightful that we were able to take this completely abstract theoretical thing of apparently no use whatsoever and find a practical application. As a result, the present generation of cryptographers all have to know algebraic number theory, which is kind of fun.Q: What is it like to be married to another mathematician?

t is the most blissful thing in the universe to be married to someone who understands what it's like to be a mathematician. In math, 99.9% of the time you spend hours, weeks, months, and years thinking about something that comes to nothing. So many times, you think you have a fantastic idea, and it goes nowhere. It is wonderful to be married to someone who understands that feeling, even if we don't always understand the details of what the other is working on.

Q: She realizes when you are lost in thought?

Yes, and she probably is too.

6. Quantum Computing Already Putting Data at Risk, Cyber Pros Agree

by James Coker
https://www.infosecurity-magazine.com/news/quantum-computing-data-risk-cyber/

Over half of organizations believe that current datasets are already threatened by future advances in quantum computing, according to a new study by Deloitte.

In the survey of more than 400 cybersecurity professionals, 50.2% of respondents said their organization is at risk of 'harvest now, decrypt later' attacks, whereby cyber-criminals extract encrypted data in anticipation of the time quantum computers are able to break existing cryptographic algorithms.

This phenomenon is known as 'Q Day,' which experts believe will occur in the next 5-10 years. Without the development of quantum secure encryption, this could potentially leave all digital information vulnerable to threat actors.

Speaking in the Q3 2022 edition of Infosecurity Magazine, Joseph Carson, chief security scientist and advisory CISO at Delinea, explained: "Quantum computing exposes a serious risk to one of the most foundational building blocks of the security industry, and that is encryption since everything in the digital world that we encrypt with a private key today will be possible to decrypt with a quantum computer in the near future."

Encouragingly, nearly half of respondents (45%) in the Deloitte survey expect their organization to complete assessments of potential post-quantum encryption vulnerabilities within the next 12 months, with an additional 16.2% predicting this process will be undertaken in the next two to five years.

However, many organizations appear to have a reactive attitude to adopting new methods of cryptography. Around a quarter (27.7%) believe advances in their organization's quantum computing security risk will most likely follow regulatory pressure to adopt legislation or policies or demand from leadership. Others admitted it would take a cyber incident, such as exfiltration of sensitive data, to drive action in this area (11.7%) or client or shareholder demand (6.8%).

Colin Soutar, Ph.D., US quantum cyber readiness leader and Deloitte Risk & Financial Advisory managing director, Deloitte & Touche LLP, commented: "It's encouraging to see that so many of the organizations with quantum computing awareness are similarly aware of the security implications that the emerging technology presents. But, it's important to note that 'harvest now, decrypt later' attacks are something all organizations – whether or not they're considering leveraging quantum computing – stand to face in a post-quantum world.

"As quantum awareness grows within boardrooms, C-suites and security teams, we're hopeful that organizations' efforts to prepare for post-quantum cyber risk management will grow as well."

Currently, work is ongoing to develop quantum-secure cryptography. The US Department of Commerce's National Institute of Standards and Technology (NIST) is in the process of selecting the encryption algorithms to become part of its planned post-quantum cryptographic (PQC) standard.

Additionally, in the Q3 issue of Infosecurity Magazine, Benjamin David investigated the world-first commercial trial of a quantum secured metro network and what this means for cybersecurity.

7. D-Wave-led Research Team Demonstrates Large-Scale Coherent Quantum Annealing

by Matt Swayne
https://thequantuminsider.com/2022/09/16/d-wave-led-research-team-demonstrates-large-scale-coherent-quantum-annealing/?utm_source=newsletter&utm_medium=email&utm_term=2022-09-25&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Making+QC+Company+List+Breaking+QC+Records+And+More+Quantum+News

D-Wave Quantum, a leader in quantum computing systems, software, and services—and the only provider building both annealing and gate-model quantum computers, today published a peer-reviewed milestone study of the first large-scale demonstration of coherent quantum annealing. The research exhibits, for the first time, dynamics of a quantum phase transition in a large-scale programmable quantum annealing processor using up to 2000 qubits in a D-Wave processor. This demonstration goes beyond the scale of any previous programmable quantum phase transition, opening the door to simulations of exotic phases of matter (unusual states of matter, outside of liquid, solid or gas, that make up the universe) that would otherwise be intractable.

The paper—a collaboration between scientists from D-Wave, the University of Southern California, the Tokyo Institute of Technology, and Saitama Medical University—entitled "Coherent quantum annealing in a programmable 2000-qubit Ising chain," was published in the peer-reviewed journal Nature Physics today and is available here. The study shows that the fully programmable D-Wave quantum processor can be used as an accurate simulator of coherent quantum dynamics at large scales. This was demonstrated showing the patterns of "kinks" separating correlated spins in almost perfect agreement with exact analytical solutions of the famous Schrodinger equation for an ideal quantum system, completely isolated from outside noise. The density and spacing of kinks depend on, among other things, the speed and "quantumness" of the experiment. Measurements of single-qubit parameters were shown to accurately predict the behavior of systems from 8 to 2000 qubits, demonstrating high levels of control in quantum simulations at all scales.

"Essentially, these experiments measured the D-Wave processor against a very well-understood quantum yardstick," said Dr. Andrew King, Director of Performance Research at D-Wave. "We found excellent agreement between theory and experiment, and that gives us a lot of confidence in our ability to manipulate programmable quantum systems, both for optimization applications and for exotic quantum simulations."

"By examining quantum dynamics on a much shorter timescale than previously thought possible using D-Wave's quantum annealers, this experiment demonstrates that these devices can operate without any discernible impact from the external environment. This opens the door to quantum simulations of models that are too large and complex to be simulated by any other means currently available," said Daniel Lidar, Viterbi Professor of Engineering and Director of the USC Center for Quantum Information Science & Technology, University of Southern California.

"This paper paves the way toward practical quantum simulations of considerable scale unexplorable by other means including classical computations," said Hidetoshi Nishimori, Professor, Institute of Innovative Research, Tokyo Institute of Technology.

"Coherence is the holy grail of quantum computing. By simulating a closed quantum system with no thermal effects at a large scale, we can glean invaluable insights into our processors' computational power and thus increase the ability to find high quality solutions for our customers," said Alan Baratz, CEO of D-Wave. "Ongoing advances in coherence times are an important priority for both our annealing and gate-model programs. The demonstration of large-scale coherence is another step towards demonstrating practical quantum advantage, and today's research is a significant step towards that milestone."

The significance of this achievement goes beyond the basic scientific aspect of understanding quantum phase transitions in one-dimensional matter. By establishing the technical basis for large-scale quantum simulations, it has paved the way for scientifically understanding the properties of a wider range of quantum materials.

Further, the scientific achievements presented in Nature Physics underpin D-Wave's ongoing commitment to relentless scientific innovation and product delivery. To date, D-Wave has brought to market five generations of quantum computers and launched an experimental prototype of its sixth-generation machine, Advantage2, in June 2022. Announced in Fall of 2021 as part of the company's Clarity roadmap, and scheduled to be available in 2023-2024, the full Advantage2 system is expected to feature 7,000+ qubits with a new qubit design, enabling 20-way connectivity between qubits in a new topology. The company also holds a broad portfolio of 200+ patents applicable to both annealing and gate-based quantum computing. And earlier this year, D-Wave opened the first Advantage™ quantum cloud service physically located in the United States, which is located at the USC-Lockheed Martin Quantum Computing Center (QCC) hosted at USC's Information Sciences Institute (ISI), a unit of the University of Southern California's prestigious Viterbi School of Engineering.

8. Rigetti Announces New Partnerships and Details Multi-Year Roadmap Designed to Reach Quantum Advantage

by Matt Swayne
https://thequantuminsider.com/2022/09/16/rigetti-announces-new-partnerships-and-details-multi-year-roadmap-designed-to-reach-quantum-advantage/?utm_source=newsletter&utm_medium=email&utm_term=2022-09-25&utm_campaign=The+Quantum+Insider+s+Weekly+Newsletter+Making+QC+Company+List+Breaking+QC+Records+And+More+Quantum+News

Rigetti Computing, a pioneer in hybrid quantum-classical computing, will share its updated multi-year roadmap today along with other notable updates regarding its partnerships and Fab-1 facility, at its inaugural investor day. The roadmap spans Rigetti's distinctive full-stack approach and is designed to help Rigetti and its partners reach critical Quantum Advantage milestones, which the Company will speak to more throughout the event.

"As a trailblazer in quantum, Rigetti is focused on delivering performance at scale to be the industry standard," said Chad Rigetti, founder and CEO of the Company. "We are making strategic, long-term investments in quantum hardware, software, and partnerships that we believe will enable us to progress toward Quantum Advantage."

"In addition, we're excited to announce several key partnerships," Rigetti continued. "These include a partnership with Bluefors to deliver new modular dilution fridges to support our planned 336Q, 1,000Q+, and 4,000Q+ quantum processing units. Earlier this week, we announced the public preview of our current 80Q Aspen-M-2 and 40Q Aspen-11 systems on Microsoft's Azure Quantum. Rigetti quantum computers are now available on the world's two largest public cloud platforms."

Keysight True-Q Error Mitigation Tools on Rigetti Quantum Cloud Services (QCS™)

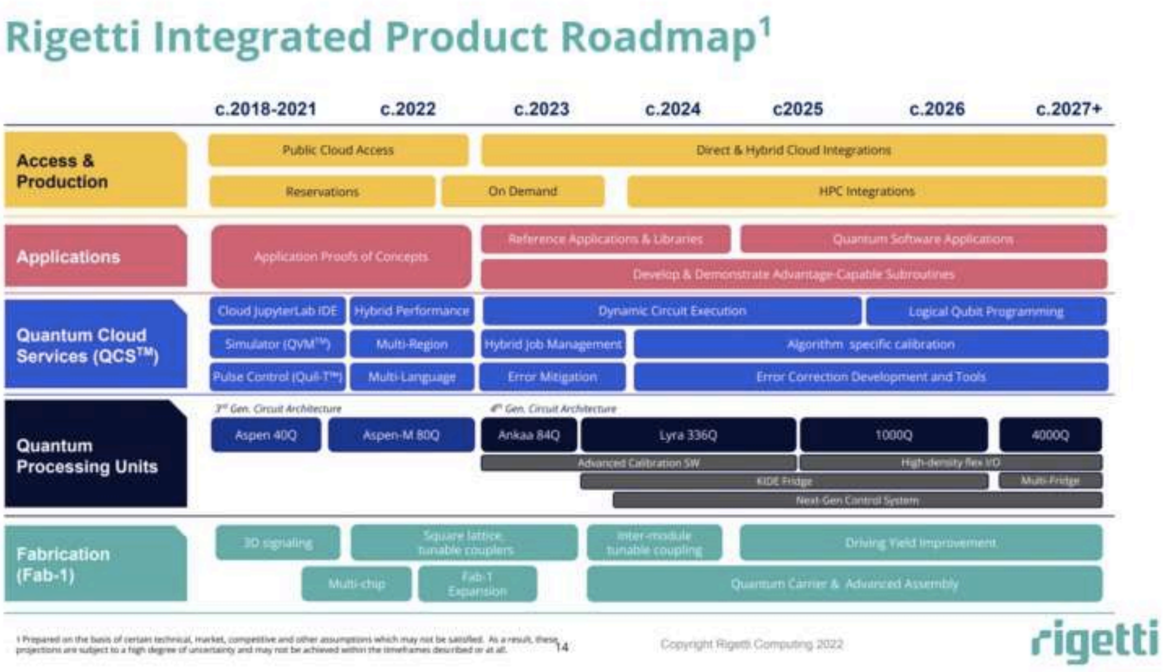
Rigetti will announce the upcoming release of Keysight's True-Q error mitigation software integrated into Rigetti QCS. This will be the first third party software tool to be integrated directly into the QCS platform, advancing the Company's partnership strategy to accelerate quantum advantage.

"Keysight's True-Q software brings a broad suite of capabilities that will help Rigetti's user base achieve higher performance quantum computing," said Joseph Emerson, Director of Advanced Research, QES at Keysight Technologies. "We have worked together to streamline access for Rigetti customers to Keysight's advanced quantum compiler technologies. I am excited to see more to come from the integration of Keysight software tools with the Rigetti platform at the forefront of the race toward quantum advantage."

Partnership with NVIDIA to Develop Hybrid GPU-QPU Workflow for Climate Modeling

Rigetti will announce a new collaboration with NVIDIA to develop a hybrid GPU-QPU workflow for climate modeling applications. The project aims to evaluate the potential for narrow quantum advantage in this research domain by applying quantum machine learning techniques in a high-performance hybrid workflow. The work builds on recent weather modeling work by Rigetti that suggested a potential for quantum advantage through this hybrid quantum-classical approach.

"Addressing challenges from an evolving climate is one of society's most important tasks, and improving our ability to model the climate is essential to make data-driven decisions," said Tim Costa, Director of HPC and Quantum Product at NVIDIA. "We are excited to partner with Rigetti to explore how combining the best of quantum and GPU accelerated computing can help address this challenge."



Rigetti Integrated Product Roadmap[1]

c.2018-2021 | c.2022 | c.2023 | c.2024 | c2025 | c.2026 | c.2027+

Access & Production
Public Cloud Access
Direct & Hybrid Cloud Integrations
Reservations
On Demand
HPC Integrations

Applications
Application Proofs of Concepts
Reference Applications & Libraries
Quantum Software Applications
Develop & Demonstrate Advantage-Capable Subroutines

Quantum Cloud Services (QCS™)
Cloud JupyterLab IDE
Hybrid Performance
Dynamic Circuit Execution
Logical Qubit Programming
Simulator (QVM™)
Multi-Region
Hybrid Job Management
Algorithm specific calibration
Pulse Control (Quil-T™)
Multi-Language
Error Mitigation
Error Correction Development and Tools

Quantum Processing Units
3rd Gen. Circuit Architecture
Aspen 40Q
Aspen-M 80Q
4th Gen. Circuit Architecture
Ankaa 84Q
Lyra 336Q
1000Q
4000Q
Advanced Calibration SW
High-density flex I/O
KIDE Fridge
Multi-Fridge
Next-Gen Control System

Fabrication (Fab-1)
3D signaling
Square lattice tunable couplers
Inter-module tunable coupling
Driving Yield Improvement
Multi-chip
Fab-1 Expansion
Quantum Carrier & Advanced Assembly

[1] Prepared on the basis of certain technical, market, competitive and other assumptions which may not be satisfied. As a result, these projections are subject to a high degree of uncertainty and may not be achieved within the timeframes described or at all.

14

Copyright Rigetti Computing 2022

rigetti

Public Preview of Rigetti Quantum Processors on Microsoft Azure Quantum

Earlier this week, Rigetti announced the release of its Aspen-M-2 80-qubit and Aspen-11 40-qubit in public preview on Azure Quantum. Rigetti's integration with Azure supports Quil, Rigetti's native quantum programming language, and Quil-T for pulse level programming. With the Azure announcement, Rigetti is now available on the world's two largest public cloud platforms.

Performance at Scale: Delivering Next-Generation Hardware in 2023

- Rigetti remains on track to deliver against its hardware roadmap in 2023 with a focus on delivering performance at scale. The upcoming Ankaa™ 84-qubit system is slated for release in early 2023, followed by the Lyra™ 336-qubit system expected in late 2023. Ankaa and Lyra will leverage Rigetti's fourth generation circuit architecture, introducing higher connectivity and tunable coupling, designed to ultimately deliver fidelities exceeding 99%. Notably, the Lyra system will bring together Rigetti advancements in scale and performance by combining Rigetti's existing multi-chip scaling technology with the fourth generation architecture.

- Rigetti will showcase plans to further expand its Fab-1 facility, which it expects to be completed late in the fourth quarter of 2022. The build-out includes an additional 5,000 square feet of clean room space for wafer manufacturing—nearly doubling its original capacity—as well as additional capabilities for performing tightly integrated cryo-microwave testing on Rigetti quantum chips.

- Rigetti has entered into a partnership with Bluefors, a leading provider of cryogenic systems, to deliver next-generation cryogenic platforms for Rigetti's upcoming 336Q, 1,000Q+, and 4,000Q+ quantum processing units. These new KIDE cryogenic platforms are expected to provide the larger size, increased cooling power, and modular design needed to support Rigetti's integrated product roadmap. Rigetti plans to take delivery of its first KIDE in early 2023, with subsequent deliveries planned for late 2023 and beyond.

9. SRM Qkrishi Quantum Centre of Excellence to Focus on Teaching and Research to help India Lead in Quantum

by Julien-Levallois

https://www.swissquantumhub.com/srm-qkrishi-quantum-centre-of-excellence-to-focus-on-teaching-and-research-to-help-india-lead-in-quantum/

Qkrishi Quantum Private Limited and SRM Institute of Science and Technology (SRMIST) have partnered to set up the SRMIST Qkrishi Centre of Excellence in Quantum Information and Computing (SQ-QuIC). SQ-QuIC was officially inaugurated today by Dr. C. Muthumizhchelvan, Vice Chancellor, SRMIST. This First of a Kind centre of excellence in a private university in India, will bring together SRM faculty, research students and Qkrishi scientists to work on cutting edge quantum algorithms and applications research. The interdisciplinary team comprising of faculty from Physics, Chemistry, Mathematics, Management and Engineering will focus on research in areas such as Finance, Drug Discovery, Logistics Optimisation, Automobile and Machine Learning. SQ-QuIC has the mission to invent and develop new technology to reshape whole industries to help India take leadership in the quantum era. SRMIST and Qkrishi will work together with industry to identify and solve the tough problems. Many industry problems have a high degree of computational complexity and are slow to converge even on the fastest supercomputers. Quantum computing brings a lot of opportunities to solve these tough problems to help humanity move forward in a sustainable way.

The partnership between SRMIST and Qkrishi will also enable students to work on cutting edge quantum technologies that will help prepare them for the quantum era. Being one of the first such labs in the world, students of SRMIST will get an opportunity to work in one of the most advanced technology areas of today. Experts have called out Quantum Computing as one of the most sought-after skills along with AI/ML, VR and Cloud.

Dr. C. Muthamizhchelvan, Vice Chancellor, SRMIST said, "Through this partnership between SRM and Qkrishi we will accelerate teaching, research, and technology development in quantum computing. SRM has always led from the front with a flexible and dynamic curriculum, exciting research and strategic partnerships to provide the best learning opportunities for the students. Now along with Qkrishi we want to be one of the first institutions in the world to bring quantum skilling, research and technology development opportunities to faculty, students, and industry collaborators

"SQ-QuIC at SRMIST Campus will help in creating a flourishing ecosystem involving faculty, students and external industry collaborators who can focus on solving some of the toughest challenges facing India and the world," said Smt. Prabha Narayan, co-founder at Qkrishi.

Shri Raghavendra V, Head of Research at Qkrishi said, "Quantum represents a new computing paradigm. Industry needs to get ready for the future of computing. Qkrishi and SRM will work to radically reshape how industry in finance, medicine and logistics work by driving innovations using quantum computing.

10. What are quantum-resistant algorithms—and why do we need them?

by Tammy Xu
https://www.technologyreview.com/2022/09/14/1059400/explainer-quantum-resistant-algorithms/

Cryptographic algorithms are what keep us safe online, protecting our privacy and securing the transfer of information.

But many experts fear that quantum computers could one day break these algorithms, leaving us open to attack from hackers and fraudsters. And those quantum computers may be ready sooner than many people think.

That's why there is serious work underway to design new types of algorithms that are resistant to even the most powerful quantum computer we can imagine.

What do these algorithms even do?

Cryptographic algorithms turn readable data into a secret, unreadable form so it can be safely shared on the open internet. They are used to secure all types of digital communication, like traffic on websites and the content of emails, and they are necessary for basic privacy, trust, and security on the web. There are several types of standard cryptographic algorithms widely used today, including symmetric-key and public-key algorithms.

Symmetric-key encryption is what people usually think of as encryption. It allows data and messages to be scrambled using a "key" so they are indecipherable to anyone without the key. It's commonly used for securing sensitive data stored in databases or hard drives. Even data breaches that compromise databases full of sensitive user information aren't as bad if the underlying data is encrypted—hackers may get the encrypted data, but there's still no way to read it.

Public-key algorithms are important too. They help get around the fundamental drawback of symmetric-key encryption, which is that you need a secure way to share symmetric keys in the first place. Public-key algorithms use a set of two keys, one that is privately kept by the recipient and one that is made public.

Anyone can use the receiver's public key to scramble data, which only the receiver can unscramble using the private key. This method can be used to transfer symmetric keys and can even be used in reverse for digital signatures—because private keys are unique to the receiver, receivers can use them to validate their identity.

Why do these algorithms need/ to be quantum resistant?

Cryptographic algorithms are able to keep data secret because they are mathematically intensive to break. It would take a modern computer trillions of years to break just one set of encryption keys using brute force.

But in the 1990s, before quantum computers were ever seriously talked about, mathematician Peter Shor discovered that the way a theoretical quantum computer would work happened to line up particularly well with cracking the kind of math used in public-key encryption.

Although no quantum computer existed at the time, other mathematicians were able to confirm that Shor's Algorithm, as it became known, could theoretically be used by such computers to break public-key encryption. Now it's widely accepted that once a working quantum computer with enough processing power is built, the algorithms we rely on today for public-key encryption will be easily breakable.

The National Institute of Standards and Technology (NIST) predicts that quantum computers that can do this may be ready in just 10 to 20 years.

Luckily, symmetric-key encryption methods are not in danger because they work very differently and can be secured by simply increasing the size of the keys they use—that is, unless mathematicians can come up with a way for quantum computers to break those as well. But even increasing the key size can't protect existing public-key encryption algorithms from quantum computers. New algorithms are needed.

What are the repercussions if quantum computers break encryption we currently use?

Yeah, it's bad. If public-key encryption were suddenly broken without a replacement, digital security would be severely compromised. For example, websites use public-key encryption to maintain secure internet connections, so sending sensitive information through websites would no longer be safe. Cryptocurrencies also depend on public-key encryption to secure their underlying blockchain technology, so the data on their ledgers would no longer be trustworthy.

There is also concern that hackers and nation-states might be hoarding highly sensitive government or intelligence data—data they can't currently decipher—in order to decrypt it later once quantum computers become available.

How is work on quantum-resistant algorithms progressing?

In the US, NIST has been looking for new algorithms that can withstand attacks from quantum computers. The agency started taking public submissions in 2016, and so far these have been narrowed down to four finalists and three backup algorithms. These new algorithms use techniques that can withstand attacks from quantum computers using Shor's Algorithm.

Project lead Dustin Moody says NIST is on schedule to complete standardization of the four finalists in 2024, which involves creating guidelines to ensure that the new algorithms are used correctly and securely. Standardization of the remaining three algorithms is expected in 2028.

The work of vetting candidates for the new standard falls mostly to mathematicians and cryptographers from universities and research institutions. They submit proposals for post-quantum cryptographic schemes and look for ways to attack them, sharing their findings by publishing papers and building on each other's different methods of attack.

In this way, they slowly weed out candidates that are successfully attacked or shown to have weaknesses in their algorithm. A similar process was used to create the standards we currently use for encryption.

However, there are no guarantees that a new type of clever quantum attack, or perhaps even conventional attack, won't someday be discovered that can break these new algorithms.

“It’s impossible to prove that you can’t break it—the nonexistence of a mathematical algorithm is hard to impossible to prove,” says cryptographer Thomas Decru. But “if something stands the test of time in the world of cryptography, the trust grows.”

11. A Retrospective Post-Quantum Policy Problem

by Herb Lin
https://www.lawfareblog.com/retrospective-post-quantum-policy-problem

In May 2022, the White House issued a National Security Memorandum that stated:

> a quantum computer of sufficient size and sophistication—also known as a cryptanalytically relevant quantum computer (CRQC)—will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions.

This concern is not new. The theoretical possibility that quantum mechanics could be used as the basis for computation was first posed in the physics literature around 1980. In 1994, Peter Shor developed an algorithm that could rapidly factor large numbers into their constituent primes if run on a quantum computer. The development and publication of Shor’s algorithm raised the possibility of undermining the RSA algorithm that underlies most secure messaging over the internet. The security afforded by the RSA algorithm is based on the difficulty of factoring large numbers, and thus Shor’s algorithm presents a potential threat to RSA.

Since 1994, the cryptography community has speculated about the forthcoming availability of quantum computing hardware that could run Shor’s algorithm. In the early days of such speculation, the range of estimates for that time frame ranged from “pretty soon” to “probably never.” However, in recent years, the emerging consensus seems to be that quantum computing, as it applies to cryptanalysis, cannot be dismissed as mere puffery. Scientific and engineering progress in quantum computing over the past 25 years has been nontrivial, and many nations are involved in supporting extensive research efforts into quantum computing. In 2016 under the Obama administration, the U.S. National Institute of Standards and Technology initiated the first public U.S. government effort to develop cryptographic algorithms that would be resistant to quantum computing. The Trump administration continued this interest in quantum computing by proposing substantial increases in funding for quantum information sciences. And, as noted above, the Biden administration’s 2022 White House National Security Memorandum has continued to emphasize the importance of quantum computing and has directed federal agencies to begin preparing for a transition.

Congress has also expressed concerns about encryption vulnerabilities that may result from quantum computing. For example, the House of Representatives passed the Quantum Computing Cybersecurity Preparedness Act in July 2022. This bill directs the Office of Management and Budget to begin the migration of U.S. government information technology systems to post-quantum cryptography a year after the National Institute of Standards and Technology issues post-quantum cryptography standards. In July 2022, a bipartisan group of senators introduced the same bill into the U.S. Senate.

These efforts have generally focused on the future by developing the technology base to support what the United States should do to ensure the security of its sensitive communications. As noted above, attention to policy regarding a post-quantum cryptography (PQC) world has been focused primarily on policy that would facilitate an infrastructural transition to quantum-resistant encryption algorithms.However, despite these efforts, policymakers have given little or no attention to what could be called a retrospective post-quantum problem. To wit—pre-quantum public-key encryption algorithms such as RSA have almost certainly been used to protect nearly all classified U.S. government messages since the 1970s, when the mathematics for public-key encryption were first discovered. A properly encrypted message is useless to anyone without the decryption key or the technology to discover that key, but even encrypted messages can be recorded for future analysis. Indeed, intelligence agencies have a habit of collecting information just in case it might be useful in the future, and there is no reason to suppose that these encrypted messages have not been recorded somewhere by some adversary government.

In a PQC world, those recorded encrypted messages will be vulnerable to decryption. In their decrypted form, they potentially hold a treasure trove of secrets. Though these are secrets from the past, decrypted messages may reveal embarrassments and dangers with potentially detrimental policy implications for today and tomorrow. The possibilities for these secrets are endless: Salacious information about a world leader currently believed to be a right and upstanding patriot to his country? Operational instructions regarding an assassination attempt or a coup supported or encouraged by U.S. authorities despite public denials? A communique about alien technology discovered by accident on the ocean floor?

As Chris Jay Hoofnagle and Simson Garfinkel rightly point out in Lawfare, even a remarkable breakthrough resulting in a quantum computer capable of factoring the large numbers characteristic of RSA public keys would not automatically undo all RSA-enabled encryption everywhere. Rather, the owner of such a computer would have to use its quantum computing resources on decrypting one message at a time. And since an encrypted uninteresting message cannot be distinguished from a similarly encrypted interesting message, it may be necessary to dedicate a significant portion of time, effort, and funding to decrypt a large volume of recorded messages before an interesting message is found.

That said, this is largely a matter of economics. The cost of PQC cryptanalysis is likely to eventually drop to a level where it makes sense to devote quantum computing resources to decrypting old, encrypted messages.

Policymakers would be wise to consider the very real possibility that in a PQC world, messages they once believed would be kept secret could in fact be made public. The adversary cannot be confident that it will be able to retrieve a large volume of interesting information from its trove of encrypted recorded messages, at least not in the immediate aftermath of a true quantum computing breakthrough. Still, the United States cannot be fully confident that any of its secrets encrypted with pre-quantum algorithms will never be revealed. Thus, the danger that such secrets will be revealed will only grow, as the adversary is able to devote more quantum computing resources to the process of retrospective decryption.

It is a common best practice for organizations to do a damage assessment in the wake of a data breach to identify what information may have been compromised and then to develop and implement a strategy to deal with that compromise. Here, policymakers have the distinct luxury of knowing that a data breach is looming in the future, even though they do not know precisely when it will occur. Every U.S. government agency that has sent a confidential message in the past should have at least a small effort devoted to developing plans for what that agency should do if and when particularly sensitive messages from the past are revealed in the PQC future.

12. SK Telecom implements post-quantum cryptography on a VPN

by SHIN HA-NEE

https://koreajoongangdaily.joins.com/2022/09/13/business/tech/Korea-SK-Telecom-SK-Broadband/20220913140222243.html

SK Telecom and SK Broadband said on Tuesday that they implemented post-quantum cryptography — which is considered secure against a quantum computer's attack — in a global virtual private network (VPN), enhancing telecommunications security.

This marks the first time in Korea for such technology to be commercially operated on an overseas network, the companies said.

Post-quantum cryptography became the latest addition to SK Telecom's quantum cryptography technologies, which include quantum key distribution (QKD) — a quantum-based method to generate a random secret key for encryption and decryption of transferred data — and quantum random number generators (QRNG), which produce random numbers for data processing using quantum mechanics.

SK Broadband, the internet provider 74% owned by SK Telecom, completed installing the post-quantum cryptography-enabled VPN in August through a software update and ran network tests in the United States, Japan and Singapore, the company said.

SK Telecom "came to hold technological capabilities to lead the whole quantum security sector with the commercial operation of post-quantum cryptography, following the QKD and QRNG technologies," Park Jong-kwan, head of the infrastructure technology division at SK Telecom, said.SK Broadband, the internet provider 74 percent owned by SK Telecom, completed installing the post-quantum cryptography-enabled VPN in August through a software update and ran network tests in the United States, Japan and Singapore, the company said.

SK Telecom "came to hold technological capabilities to lead the whole quantum security sector with the commercial operation of post-quantum cryptography, following the QKD and QRNG technologies," Park Jong-kwan, head of the infrastructure technology division at SK Telecom, said.

13. CISA Directs Critical Infrastructure Organizations to Prepare for Post-Quantum Cryptography

by ALICIA HOPE

https://www.cpomagazine.com/cyber-security/cisa-directs-critical-infrastructure-organizations-to-prepare-for-post-quantum-cryptography/

The Cybersecurity and Infrastructure Security Agency (CISA) published guidelines that critical infrastructure organizations should adopt for a smooth migration to post-quantum cryptography standards. The National Institute of Standards and Technology (NIST) will publish these standards in 2024.

Meanwhile, CISA's advisory enumerates the potential impact of quantum computing and recommends actions that critical infrastructure and government network operators should take.

CISA made the recommendations after analyzing 55 National Critical Functions (NCFs), their quantum vulnerabilities, and steps to mitigate the security weaknesses to facilitate a smooth transition to post-quantum cryptography.

The DHS and NIST also published a roadmap document with actionable insights for transitioning to the new cryptographic standards. CISA recommends its Preparing Critical Infrastructure for Post-Quantum Cryptography insight document and DHS' Post-Quantum Cryptography Roadmap.

What is quantum computing and its risks?

Quantum computers are devices with higher computing capabilities recorded up to 158 million times faster than today's most powerful supercomputers. Their extreme computing capabilities would allow them to solve complex mathematical functions used by modern encryption algorithms.

Experts predict quantum computers will break asymmetric encryption algorithms, such as RSA, that rely on public key exchange between communicating applications. However, symmetric encryption algorithms, such as AES, that depend on a single secret key known by both the sender and receiver can weather quantum computing by using longer secrets.

While quantum computing power will be economically beneficial, it also threatens the safety and integrity of data protected with public key algorithms.

"While post-quantum computing is expected to produce significant benefits, we must take action now to manage potential risks, including the ability to break public key encryption that U.S. networks rely on to secure sensitive information," said Mona Harrington, acting Assistant Director National Risk Management Center, CISA.

Quantum computing threatens critical infrastructure and national security

Given its immense computing power, quantum computing will break public key cryptography algorithms that protect sensitive data related to NCFs.

Private companies and nation-state actors, including those interested in cyber espionage, seek dominance in quantum computing.

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

According to the Secretary of Homeland Security Alejandro Mayorkas, the post-quantum cryptography transition was a priority for cybersecurity resilience.

However, CISA states, "quantum computing technology capable of breaking public key encryption algorithms in the current standards does not yet exist." Thus, businesses and critical infrastructure operators can conveniently transition to post-quantum cryptography before this emerging technology proliferates.

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

CISA identified 55 NCFs connecting, distributing, managing, or supplying critical goods or services. Each entity faces specific risks from quantum computing's ability to break modern encryption standards.

"NCFs are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or a combination thereof," CISA wrote.

Post-quantum cryptography transition bottlenecks

CISA stated that the dependence on geographically dispersed and vulnerable industrial control systems would challenge the post-quantum cryptography transition process. This situation would affect many critical infrastructure organizations that depend on IoTs, including ICS.

CISA listed 18 NCFs that depend on ICS, including water supply, electricity generation, distribution, and transmission entities, transportation, and management of hazardous materials.

NFCs with long secrecy lifetimes face huge risks from quantum computing and would require continued support in the post-quantum computing universe. Such organizations operate on confidential data stored over long periods, such as trade secrets and personal and health information.

The agency enumerated nine NCFs dealing with long secrecy lifetime information, including law enforcement, community health, internet communications, wireless access networks, defense support, and medical records access systems.

CISA warned that threat actors used "catch-and-exploit campaigns" involving collecting encrypted data and storing it for future exploitation when quantum computers break current cryptography algorithms.

However, CISA noted that migrating some priority NCFs to post-quantum cryptography standards would support the migration of others, thus mitigating the risk posed by quantum computing.

DHS' post-quantum cryptography transition recommendations

The DHS post-quantum cryptography roadmap recommended engaging with standards development bodies and taking inventory of critical data and cryptographic technologies.

Similarly, organizations should identify areas where public key is being used and label such systems as vulnerable.

Lastly, organizations should prioritize systems for replacement based on the following factors.

- Whether the system is a high-value asset
- The nature of other systems it protects and communicates with
- The extent the system shares information with federal and external entities
- Whether it supports critical infrastructure
- How long the data requires protection

CISA's Insight document follows the federal government's National Quantum Initiative in 2018 to accelerate quantum research and development for economic development and national security.

In May 2022, the Biden administration issued the National Security Memorandum 10 that, among other things, required advancing the adoption of quantum-resistant cryptography.

U.S. legislators also introduced the Quantum Computing Cybersecurity Preparedness Act in the House in April and passed it in July 2022. The bill seeks to address the migration of executive agencies' information systems to post-quantum cryptography.

14. How to prepare for post-quantum computing security

by Kyle Johnson

https://www.techtarget.com/searchsecurity/feature/How-to-prepare-for-post-quantum-computing-security

A post-quantum security world sounds scary. Quantum computers are projected to break many of the cryptographic standards that have adequately protected data for decades.

While companies don't need to hit the panic button over quantum quite yet -- it will likely be decade or more before the technology is ready -- that doesn't mean quantum should be ignored.

President Joe Biden signed two quantum computing presidential directives in 2022, signaling the time is now to figure out how to handle the emerging technology. The directives call for the creation of quantum-resistant cryptographic standards -- a task NIST has been busy with for more than half a decade -- and preparing federal agencies to adopt these future standards.

Companies need to figure out how they will be affected once quantum computing arrives, which may call for better data protection now or preparing for post-quantum cryptography (PQC).

The quantum security worry

The major concern with quantum computing is how easily it will crack data transmission cryptography algorithms. The asymmetric RSA algorithm, for example, which is based on integer factoring and provides sufficient security on classical computers, will be breakable on quantum computers.

Attackers are aware of this issue and have begun to do what is known as data scraping -- collecting encrypted data in hopes it will be useful later. Because storage is cheap, attackers are harvesting encrypted data now to crack once quantum computing matures.

How to prepare for PQC security

Heather West, research manager at IDC, is also advising organizations to start looking at quantum. "Piecemealing it together now is going to be a lot easier than suddenly going, 'Oh my goodness, the technology is here, what do we do?'" she said.

To prepare and make future transitions easier once PQC becomes standardized, companies should consider the following three steps.

1. **Inventory and classify data**

   This step involves reviewing data and deciding what is considered sensitive. Conduct a data inventory to understand what data your company has and its data classification to understand what data needs which protections.

   Be sure to consider what data needs stronger protection now in terms of the data scraping threat.

"What data is OK four years from now that I am not worried about someone scraping?" said Christopher Savoie, CEO of Zapata Computing. "On the other hand, what would I be worried about for years?" Such data could involve corporate or trade secrets and other business-critical information. Take the appropriate actions to ensure data is safe now and in the future.

2. **Understand future exposure**

   With data inventoried and classified, consider how data is currently protected and whether it will be at risk once quantum computing arrives.

   "Organizations should start looking at their potential exposure to understand what their reliance on cryptography is," said Colin Soutar, managing director at Deloitte & Touche LLP. "It might be deeply embedded in third-party tools; it might be proprietary, transactional capabilities. You need a sense of where cryptography is embedded into your systems and how data is being protected."

   Soutar noted that examining cyber hygiene around current data could help beyond preparing for PQC.

   "Even if you end up doing nothing around the potential future quantum risk, maybe you identify SSL certificates that are outdated or something else that is more perfunctory and needs to be updated," he said.

3. **Create a mitigation strategy**

   With data inventoried and potential exposure understood, the next step is to create mitigation groups and mitigation strategies.

   "Using a mitigation group, start looking at what policies and procedures need to be in place for when the inevitable happens," Savoie said.

   This should include a data security policy, incident response plan and business recovery plan, at a minimum. This step also involves assessing what company data might already be exposed and stored by attackers and determining how to handle that situation. Next, organizations should look at the critical data they have stored now and decide whether it needs additional layers of encryption to protect it.

   Symmetric encryption, commonly used by organizations to keep stored data secure, won't be largely affected by quantum computing. Grover's algorithm, which demonstrates how quantum computing will quadratically speed up database searches, has shown it halves the time needed to break symmetric encryption. NIST therefore recommends organizations use at least AES-192 or AES-256 to encrypt stored data.

   Data in transit, however, is at risk of being broken by quantum computing. To counter this, organizations will need to adopt PQC encryption standards to replace asymmetric algorithms. NIST is evaluating several options, two of which -- SIKE and Rainbow -- were easily defeated by classical computers, so stand no chance against quantum computers. NIST is still evaluating seven potentially viable options.

Handling asymmetric encryption changes plays into the last aspect of mitigation, Savoie added. This means organizations need to start thinking about how to remain crypto-agile.

"As standards change going forward, we need to ensure infrastructure is in a place where we can actually adapt to new threats and new technologies to mitigate those threats," Savoie said. "Getting your systems crypto-agile and forward-compatible to new standards takes time and is something you need to start working on now."

PQC implementation options

Three options have been bandied about as experts work to figure out the most effective PQC option for quantum security preparation.

First, follow NIST's research and consider any algorithms it vets. Currently, four primary finalist algorithms remain uncracked and potentially viable. Three additional algorithms also are being studied for viability.

Another option is quantum key distribution (QKD), which uses quantum mechanics to securely exchange encryption keys. Data encrypted via QKD creates a random quantum state that is difficult to copy. Many QKD protocols can also detect eavesdroppers. The National Security Agency, however, has stated this option is not viable on its own as it now stands.

A third option is to combine PQC encryption standards and QKD, suggested Rik Turner, principal analyst at Omdia. This would make it more difficult for attackers, he noted, because they would need to break through both encryption and QKD to access data in transit.

15. Most educational institutions store sensitive data in the cloud. Is it safe?

by Help Net Security
https://www.helpnetsecurity.com/2022/09/09/educational-institutions-cyberattack/

A Netwrix survey revealed that 47% of educational institutions suffered a cyberattack on their cloud infrastructure within the last 12 months. For 27% of them, incidents in the cloud were associated with unplanned expenses to fix security gaps.

“Educational institutions are keen to broaden their cloud adoption: The sector expects to have 56% of the workload to be in the cloud by the end of 2023, compared to this year’s 44%,” comments Dirk

Schrader, VP of Security Research at Netwrix.

"But without proper visibility into who has access to sensitive data and when and how that data is being used, IT teams will not be able to proactively mitigate data overexposure and spot suspicious behavior in the cloud."

What makes educational institutions susceptible to a cyberattack?

83% of educational organizations confirmed they store sensitive data in the cloud. With educators and students constantly sharing that information, they are more concerned about insider threats than other industries. 48% of respondents in this sector consider cybersecurity risks associated with their own employees to be the biggest ones.

"The educational sector has a good reason to be concerned about insider threats since 42% of them experienced account compromise attacks in 2022 compared to the average of 31% from the other industries surveyed. Accordingly, their IT teams should pay closer attention to identity and access management by implementing a zero standing privilege approach and enforcing strong password policies," adds Schrader.

16. QuSecure's Post-Quantum Cybersecurity Solution Named Winner of 2022 New Product of the Year Award as Best Quantum Cybersecurity Solution

by James Dragon
https://thequantuminsider.com/2022/09/08/qusecures-post-quantum-cybersecurity-solution-named-winner-of-2022-new-product-of-the-year-award-as-best-quantum-cybersecurity-solution/?utm_source=newsletter&utm_medium=email&utm_term=2022-09-25&utm_campaign=The+Quantum+Insiders+Weekly+Newsletter+Impressive+Valuations+Important+Collaborations+Interesting+Investigations+And+More+Quantum+News

TQuSecure™, a leader in post-quantum cybersecurity (PQC), today announced that QuProtect™, the industry's first end-to-end PQC software-based solution uniquely designed to protect encrypted communications and data with quantum-resilience using quantum secure channels, has won the 2022 New Product of the Year Award from Security Today magazine, the leading industry media brand providing technology, education and solutions for security professionals; and securitytoday.com, the preeminent editorial website for the security industry. QuProtect was recognized as the winner in the Quantum Cybersecurity awards category.

For the past 14 years, the Security Today New Product of the Year Awards have honored the out-standing product development achievements of security equipment manufacturers whose products are particularly noteworthy in their ability to improve security.

"The PQC sector is rapidly gaining a lot of attention, and it's an honor for QuProtect to be designated as the industry's best Quantum Cybersecurity solution with this New Product of the Year Award," said Skip Sanzeri, QuSecure Founder and COO. "Our QuProtect solution will enable organizations to protect their encrypted data and secure private information, as the world accelerates toward a quantum future, including quantum computing's ability to break our current encryption. QuProtect uniquely combines QuSecure's post-quantum technologies providing secure, interoperable cybersecurity to protect networks from today's classical threats and future quantum threats."

QuProtect enables organizations to leverage quantum resilient technology for the first time to help prevent today's cyberattacks, while future-proofing networks and preparing for post-quantum cyber threats. It provides quantum-resilient cryptography, anytime, anywhere and on any device. QuProtect uses an end-to-end quantum-security-as-a-service (QSaaS) architecture that addresses the digital ecosystem's most vulnerable aspects, uniquely combining zero-trust, next-generation post-quantum-cryptography, quantum-strength keys, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed around the entire data lifecycle as data is stored, communicated and used.

"After hosting this New Product of the Year program, I was struck with the intense effort by manufacturers, who exceeded last year's entries. We are fortunate to have so many entries and applaud every entry for the ingenuity and painstaking efforts to ensure the security business is meeting the technology challenges," said Ralph C. Jensen, editor in chief of Security Today magazine. "New Product of the Year confirms to me that the best and the brightest are completely invested in their craft and have strategic plans to bring new technology to the forefront."

QuProtect is the industry's most advanced PQC solution providing quantum resilience for many of today's critical use cases, including network, IoT, edge devices and even satellite communications. QuProtect can be hosted on-premise or via the cloud delivering the most compatible solution to the post-quantum problem, solving today's complex compliance challenges, such as bring-your-own-device (BYOD) and work-from-home policies. An organization can implement PQC across all devices on the network with minimal disruption to existing systems, protecting against current classical and future quantum attacks which could irreparably disrupt industries and infrastructures across government and commercial sectors.

17. NSA Releases Post-Quantum Algorithms, Aims for Full Implementation by 2035

by Alexandra Kelley

https://www.nextgov.com/cybersecurity/2022/09/nsa-releases-post-quantum-algorithms-aims-full-implementation-2035/376880/

The National Security Agency became the latest federal agency to begin its digital migration to quantum-resistant networks, as the emerging technology poses major cybersecurity threats to unprepared digital systems.

Released in an advisory document on Wednesday, NSA officials notified National Security Systems owners and vendors of the future post-quantum algorithmic requirements needed on classical networks that harbor sensitive data related to national security.

"This transition to quantum-resistant technology in our most critical systems will require collaboration between government, National Security System owners and operators, and industry," said NSA Cybersecurity Director Rob Joyce. "Our hope is that sharing these requirements now will help efficiently operationalize these requirements when the time comes."

The NSA's new encryption standards are outlined in its Commercial National Security Algorithm Suite 2.0, denoted as CNSA 2.0. The upgraded algorithm includes new public and symmetric key encryption and software and firmware updates. CNSA 2.0 algorithms were analyzed and deemed secure against classical and quantum computers.

Officials are releasing these algorithms now to encourage entities using NSS to plan and budget their post-quantum cryptographic systems migrations.

"We want people to take note of these requirements to plan and budget for the expected transition, but we don't want to get ahead of the standards process," Joyce added.

NSA further noted that there will be a transition period for all NSS participants, and that NSS owners and operators shouldn't deploy the new quantum-resistant algorithms until they have been approved by officials at the National Institutes of Standards and Technology and National Information Assurance Partnership.

Post-quantum encryption has been an increasingly popular requirement for public systems, as nations race to develop a viable quantum computer, which stands to be significantly more powerful than classical computers. NIST had previously identified four quantum-resilient algorithms in July to help both public and private networks prepare for the advent of quantum computing.

Dustin Moody, a mathematician at NIST, has been at the helm of the agency's efforts to develop more post-quantum cryptographic algorithms. He said that the steps the NSA announced appear reasonable and that they were looking to partner with NIST to standardize the quantum-resistant algorithms.

He also appreciated the note to wait for accompanying standards to be published before implementing the algorithms, and that NSA's timeline of complete quantum-resistant algorithm implementation among NSS owners by 2035 works with President Biden's national security memo.

"I hope their announcement continues to increase awareness of the transition to PQC [post-quantum cryptography] algorithms," Moody told Nextgov.

18. NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems

https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

The National Security Agency (NSA) released the "Commercial National Security Algorithm Suite 2.0" (CNSA 2.0) Cybersecurity Advisory (CSA) today to notify National Security Systems (NSS) owners, operators and vendors of the future quantum-resistant (QR) algorithms requirements for NSS — networks that contain classified information or are otherwise critical to military and intelligence activities.

A cryptanalytically-relevant quantum computer (CRQC) would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used today. Given foreign pursuits in quantum computing, now is the time to plan, prepare and budget for a transition to QR algorithms to assure sustained protection of NSS and related assets in the event a CRQC becomes an achievable reality.

"This transition to quantum-resistant technology in our most critical systems will require collaboration between government, National Security System owners and operators, and industry," said Rob Joyce, Director of NSA Cybersecurity. "Our hope is that sharing these requirements now will help efficiently operationalize these requirements when the time comes."

The Director of NSA is the National Manager for NSS and therefore issues guidance for NSS. The algorithms in CNSA 2.0 are an update to those in the currently required Commercial National Security Algorithm Suite (now referred to as CNSA 1.0) listed in CNSSP 15, Annex B (released in 2016). The CNSA 2.0 algorithms have been analyzed as secure against both classical and quantum computers, and they will eventually be required for NSS.

NSA's CNSA 2.0 algorithm selections were based on the National Institute of Standards and Technology's (NIST) recently announced selections for standardization for quantum-resistant cryptography, but there are neither final standards nor FIPS-validated implementations available yet.

NSA urges NSS owners and operators to pay attention to NIST selections and to the future requirements outlined in CNSA 2.0, while CNSA 1.0 compliance continues to be required in the interim.

"We want people to take note of these requirements to plan and budget for the expected transition, but we don't want to get ahead of the standards process," said Joyce.

NSS owners and operators should not deploy QR algorithms on mission networks until they have been vetted by NIST and National Information Assurance Partnership (NIAP) as required in CNSSP-11. There will be a transition period, and NSA will be transparent about NSS transition requirements.

For additional information, the CNSA 2.0 CSA is accompanied by a cybersecurity information sheet (CSI), "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ." This CSI provides updated answers to quantum-related FAQs that were previously published on NSA's website.

19. NIST Issues Call for Additional PQC Digital Signature Algorithms

https://quantumcomputingreport.com/nist-issues-call-for-additional-pqc-digital-signature-algorithms/

As mentioned in our article last month about NIST' Round 3 selection for Post Quantum Cryptography (PQC) algorithms, they are now formally issuing a call for additional PQC algorithms to use for digital signatures. In Round 3, they did select CRYSTALS-Dilithium, Falcon, and SPHINCS+ for use as quantum resistant digital signatures. CRYSTALS-Dilithium and Falcon are based upon a structured lattice class of algorithms while SPHINCS+ uses a stateless hash-based signature scheme. However, weaknesses were found in Rainbow and a few other algorithms and they were eliminated from further consideration. As a result, NIST has no additional digital signature candidates to evaluate during Round 4. For comparison, NIST selected four Key Encapsulation/Encryption algorithms for evaluation in Round 4 and potential future standardization.

NIST is concerned that the three digital signature algorithms selected in Round 3 do not provide enough diversity for protection against possible weaknesses that might be found in the future. Their primary interest is to identify general-purpose signature schemes that are not based on structured lattices. And for certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification. Although NIST won't reject out of hand a submission of a new lattice based algorithm, it would need to provide a considerable improvement in either performance or security properties over CRYSTALS-Dilitihum and Falcon to be considered.

NIST has established a final deadline of June 1, 2023 for parties to submit new digital signature algorithms for consideration. But they also indicated that any submission packages submitted by March 1, 2023 will be reviewed for deficiencies with a notification by March 31, 2023 if any are found. This would provide the submitter with about 60 days to correct any deficiencies before the final deadline. You can view a summary of NIST's Call for Proposal on a web page here and the detailed document describing their criteria and procedures for making a submission here.

20. Researchers publish post-quantum upgrade to the Signal protocol

by Help Net Security
https://www.helpnetsecurity.com/2022/09/07/post-quantum-cryptography-signal-protocol/

PQShield published a white paper that lays out the quantum threat to secure end-to-end messaging and explains how post-quantum cryptography (PQC) can be added to the Signal secure messaging protocol to protect it from quantum attacks.

The company is offering to license its end-to-end encrypted messaging IP to the Signal Foundation pro bono – if/when they plan to upgrade their system – to support the non-profit behind the free encrypted messaging app, Signal, in its mission to make secure communication accessible to everyone.

Popularity of secure messaging apps

The widespread adoption of smartphones in the last decade has brought with it a meteoric rise in the use of secure messaging apps. Over 2 billion people used WhatsApp in January 2022, and 40 million people used Signal. But however secure these messaging apps are today, large-scale quantum computers will soon have the processing power to break the end-to-end encryption they rely on to keep messages private.

The issue is compounded by the prospect of a "harvest now, decrypt later" attack. Threat actors could already be gathering and storing encrypted messages today, with a view to decrypting them at a later date, with potentially devastating consequences.

Adding post-quantum cryptography to the Signal protocol

Thomas Prest, Lead Cryptography Researcher at PQShield said: "The Signal protocol is widely regarded as the gold standard for secure instant messaging. However, the cryptographic problem underlying its security is known to be easily solvable by quantum computers, and any adversary harvesting current communications would easily be able to decrypt exchanged messages in the future. That's why we are publishing our full analysis, research and solutions for how to protect secure instant messaging from the quantum threat. The stakes are just too high not to do so."

Adding post-quantum cryptography to the Signal protocol – considered the gold standard for establishing secure messaging between two parties – would not be without technical challenges. There is a pressing need to build quantum-secure solutions that mimic the functionality and security guarantee of the Signal protocol's existing key components.

"Secure messaging has become almost a fundamental right for much of the global population. It's how many businesses communicate, how whistleblowers share truth with journalists, and how family and friends connect across borders. As one of the most common forms of end-to-end encryption, secure messaging is particularly vulnerable to the quantum threat," said Ali Kaafarani, CEO at PQShield.

"The PQShield team has worked hard to set out the security and performance challenges for secure messaging in such a way that all the leading messaging apps could become quantum-secure in a reasonable timeframe. We're proud to offer this advisory for free, so private communication can remain accessible to all," Kaafarani concluded.

21. Government Seeking Quantum-Proof Encryption

by Meredith Roaten
https://www.nationaldefensemagazine.org/articles/2022/9/6/government-seeking-quantum-proof-encryption

Once matured, quantum technology is expected to create a shift in the defense world due to the large volume of data it will be able to quickly process. While that can lead to great advances in science and technology, it can also empower those seeking to break into encrypted communications.

The Department of Commerce recently identified four algorithms that could stymie quantum hackers.

The National Institute of Standards and Technology recently announced it had completed a major step in its effort to create guidelines for encryption that protect against quantum-based attacks. Experts said the algorithms present an opportunity for federal agencies to begin evaluating what security measures work best for them.

The institute has been pitting cryptographers against each other for six years to come up with a new standard for encryption. The selected algorithms — CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON and SPHINCS+ — are just the first step in a long road to complete safety from quantum computing, said Duncan Jones, head of cybersecurity at Quantinuum, a quantum computing firm based in Colorado.

"It makes it much easier to start planning and testing, which is important because there is so much work to do ahead of us," he said.

Pete Ford, senior vice president for government operations at Silicon Valley-based cybersecurity company QuSecure, described the severity of the quantum threat as the next international arms race for the defense industry.

If quantum computers unlock the information secured by current encryption technology, adversaries could gain access to U.S. operational plans, ally partnership strategies and more, he said.

"We really appreciate the freedom that our information technology allows us. When that's taken away, it's really hard to capture that freedom back," he said.

Of the nearly 70 algorithms that were submitted for consideration to become part of the standard, "simplicity and elegance" seem to be characteristics favored by NIST, Duncan said.

"Where it was a more easily understood algorithm, the more confident I think they felt in selecting it," he said.

Faster and smaller algorithms were also favored, he noted. CRYSTALS-Kyber has "comparatively small encryption keys" and quick speed, according to a press release about the standard. CRYSTALS-Dilithium and FALCON will be used for protecting digital signatures, which are used for identity authentication. They were praised for their "high efficiency" by NIST reviewers.

The way asymmetric cryptography, or public key encryption, works is by creating one public and one private key. The keys are mathematically linked using an algorithm. People can exchange public keys in order to decrypt, or unscramble, the secure communications they are exchanging.

The encryption is safe because it would take hackers too long to guess the key using a traditional computer. But if a hacker leverages the processing power of quantum, it renders the key much easier to understand, bypassing the encryption and gaining access to protected communications.

Ford said QuSecure has already been using some of the algorithms that are part of the new standard. For example, the company demonstrated secure communications for a government client using CRYSTALS-Kyber earlier in the summer.

During the demonstration, the company turned on a post-quantum communications channel over the open internet in a combined Air Force, Space Force and North American Aerospace Defense Command facility and demonstrated the use of quantum-resilient keys.

Ford said it was the first time a quantum-protected line of communication had been opened in a government facility.

Using the algorithm and tunnel to protect communications didn't introduce any new latency or bandwidth issues, he said.

Jones added because so many nations are racing to develop quantum technology, it is possible a researcher may develop new techniques to break encryption. That could mean adversaries could start decrypting communications even faster.

"Agencies need to treat this threat seriously and recognize that the attacks may have begun," he said.

In addition to experimenting with new algorithms, agencies need to become crypto-agile, he said. The ability to adapt will ensure long-term protection.

"We want to be able to change algorithms in the future without a huge headache," he said. "And anytime we find a system that was painful to change this time around, we should make it easier in the future."

That's one reason why the SPHINCS+ algorithm is an "unexpected" but valuable choice, Jones noted. Because it is from a different family of algorithms than FALCON and CRYSTALS-Dilithium — meaning it is based on a different type of math — it can work as a backup to the others, according to a press release.

NIST is also reviewing an additional four algorithms, a statement said. The announcements for the standard were separated into two because of the "need for a robust variety of defense tools," according to the institute.

Jones emphasized that though quantum computing is a serious risk for federal agencies and companies who work with the government, it can still be an "ally" to cybersecurity. Because of its yet unrealized processing power, it could be used to help make algorithms harder to crack, he said.

"We're going to get past the threat phase, and then all that will be left will be the benefits that quantum can bring," he said.

22. 5 Ways to Prepare Now for Quantum Computing

by Tim Callan
https://sectigo.com/resource-library/5-ways-to-prepare-now-for-quantum-computing

For nearly 50 years, public key infrastructure (PKI) has provided a secure cryptographic foundation for the world's data. But in the next few years quantum computers are destined to render obsolete the current cryptographic algorithms that secure devices and the people who use them.

PKI relies primarily on two standardized algorithms, Rivest-Shamir-Adleman (RSA) and elliptic-curve cryptography (ECC), which act as the "digital trust stamps" to verify the massive amounts of human and machine identities accessing data every second. However, these algorithms are soon to be easily broken by quantum computers. If an average computer today tried to break a message using standard encryption, it would take about 300 trillion years. A quantum computer will be able to do the same thing in a week. The potential impact of quantum computing is so serious, that it's sometimes known as The Quantum Apocalypse.

Preparation is well underway. For the past six years, the US National Institute of Standards and Technology (NIST) has been conducting a competitive search for post-quantum encryption algorithms. In a milestone July announcement, NIST released its winning selections: CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.

There is still much work left to be done to standardize these algorithms (which isn't expected to be complete until 2024), and a quantum computer capable of breaking today's encryption hasn't been created yet. However, enterprises – government and private industry alike – need to start planning now for fast, efficient, and error-free deployment to new cryptographic standards. In fact, the Cybersecurity and Infrastructure Security Agency recently released a bulletin listing key actions for IT to begin working on right away. **Here are five things IT teams can do today to protect their enterprises from quantum-based breaches**:

- **Take inventory.** The place to start is by taking inventory of all encrypted systems and preparing a strategy for deployment of the new cryptography. From the ground up, understand where the most important systems are, what the risks are, what the use cases are, who is involved in this transition, and what systems will likely be affected by quantum computing. The unknown becomes a vulnerability.

- **Test the new post-quantum cryptographic algorithms.** It's not possible to issue a public certificate with these new algorithms yet because they're not standardized, and current software won't support them. Vendors, software, OS, and service providers are now starting to gear up to support these primitives, and until that happens, enterprises can't use them in production. However, it is possible to start testing the algorithms in lab environments. IT professionals should test the new cryptography in controlled environments, while the standards work is being done. Everyone must understand how to use new certificate types like hybrid certificates and what private Certificate Authority (CA) software capable of using post-quantum algorithms looks like. Sectigo Quantum Labs offers a free hybrid certificate toolkit for security professionals to evaluate their post-quantum options.

- **Create a plan for transitioning systems.** Every use case for post-quantum cryptography will likely involve a host of interdependent technologies. Enterprises must understand the intricate systems in place and have a plan for transitioning them to post-quantum cryptography.

  Some systems won't be able to consume the new types of quantum-safe certificates, which begs the important question: How much risk is associated with that old system? If the answer is "too much," then IT leaders must decide if it can be decommissioned. The only other option is to leave the systems running while vulnerable to attack from quantum computers. Depending on the nature and sensitivity of the data and operations involved, leaders will have to make pragmatic choices about the best paths forward.

- **Work with vendors.** It's time to work hand-in-hand with the vendor community. For almost all the enterprises in the world, the vast majority of the post-quantum cryptography implementation must be done by vendors. Hardware, software, and service providers will deliver products to enterprises. Then it's the IT leader's job to implement these new post-quantum-ready solutions and integrate them intelligently. Today IT leaders should already be finding out how their technology vendors plan on supporting the new post-quantum cryptographic algorithms.

- **Educate your workforce.** The average sysadmin, rightfully so, is not currently thinking about a post-quantum world in a meaningful way. After all, he or she is consumed with keeping the lights on today. Two years may seem like a long time away, but technology teams are well advised to begin today in taking inventory and understanding the impact of this computing progress.

In addition to testing algorithms in sandboxes, speaking with vendors, and determining what their post-quantum infrastructure should look like, they can take inventory of those within their organizations who will be affected and provide training on how to interact with those new systems.

Enterprises can't wait. Be proactive and start preparing now, because it's going to take time to switch to quantum-safe cryptography.

23. A new 380 km-long intercity QKD infrastructure in Poland

by Catherine Simondi

https://www.idquantique.com/a-new-380-km-long-intercity-qkd-infrastructure-in-poland/?utm_term=A%20new%20380km-long%20intercity%20QKD%20infrastructure%20in%20Poland&utm_campaign=Quantum%20Era%20Security%20Times%20September%202022&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%20September%202022-_-A%20new%20380km-long%20intercity%20QKD%20infrastructure%20in%20Poland

Poznań Supercomputing and Networking Center (PSNC) and ID Quantique (IDQ) collaborate once again to establish a new Quantum Key Distribution (QKD) link between Poznan and Warsaw. This link will provide new services for a number of applications such as telemedicine, medical data transmission, data storage and public services.

National Laboratory for Photonics and Quantum Technologies – project aiming at developing a country-wide quantum communication infrastructure. This infrastructure will initially enable research and development work on QKD and investigate its integration with other mechanisms currently used to secure data transmitted over IT and telecommunication systems. It will later lead to the design, launch and development of complex and secure systems for real-world applications.

QKD technology is currently being tested and introduced in the best research centers in Europe and in the world. It is already used by leading companies and governments to secure data in motion. Sending QKD keys to third party cryptographic systems is an example of the safest known method of communication. Quantum technology can be used today for securing internet connections, from smartphones and computers to datacenters, and to provide safe services to end-users.

In this installation, IDQ deployed their Cerberis XG series, the fourth generation of QKD systems, on the PIONER – Polish National Research and Education – network operated by the PSNC. The goal of the PSNC is to further integrate its local metro QKD infrastructure, which was developed last year in Poznan, with this new long-distance Poznan-Warsaw QKD link. The final goal is to interconnect all High Performance Computing Centers in Poland and to establish common access layers to QKD services. This will provide access hubs for different use cases and connected applications, such as: telemedicine, medical data transmission, data storage, and public services provided by local administration units. Selected nodes will act also as possible cross-border QKD infrastructure nodes, which will open new possibilities for international QKD infrastructure and services. This pan-European aspect is especially important as PSNC and the PIONIER network are part of the European Research and Education Community.

> *Launching the QKD link between Poznan and Warsaw is the first stage to building a nationwide quantum communication network, providing access to modern technology to companies and organizations seeking to protect their assets in the post quantum era.*
>
> Artur Binczewski, Director of Network Technologies Division at PSNC

> *This is the first large-scale national deployment in Europe and we feel honored to support Poznań Supercomputing and Networking Center once again to help them offer new secured services to their customers in Poland, with the aim of extending internationally in the near future.*
>
> Grégoire Ribordy, CEO and co-founder of ID Quantique

24. Low-Power Cryptographic Smart Chip Senses, Stores, Computes, and Secures Data

by Cabe Atwell

https://www.hackster.io/news/low-power-cryptographic-smart-chip-senses-stores-computes-and-secures-data-f8264e7765c5

In our modern world, we are surrounded by sensors that continuously collect, consume, store, and communicate a huge volume of information — information that is increasingly vulnerable to theft and misuse. IoT edge sensors tend to operate with limited hardware resources and at low energy budgets, making it difficult to implement ciphering algorithms. A solution proposed by researchers at Penn State, led by Saptarshi Das, demonstrates an "all-in-one" 8 x 8 area of robust, low-power, bio-inspired crypto engines that can integrate with IoT edge sensors, enabling data encryption.

Since silicon, which is commonly used to make cellphone transistors, would not be able to build a transistor small enough to limit energy use, the team turned to 2D materials. Specifically, they turned to molybdenum disulfide or MoS2, a material less than one nanometer thick, to create a low-power cryptographic chip.

Basing the chip design on MoS2, Penn State's smart hardware platform mitigates energy consumption while adding a layer of security. Exploiting the optoelectronic sensing and in-memory computing capabilities of 2D memtransistors based on photosensitive monolayer MoS2, it is possible to introduce near sensor and robust security solutions for IoT edge devices with minimal hardware investments and frugal energy expenditure. 2D memtransistors are three-terminal devices rather than two, and their additional gate terminal allows both nonvolatile and analog programming of the conductance states as well as electrostatic control of the 2D channel.

The chip design employs three hundred and twenty MoS2 transistors, each of which has a sensing unit, a storage unit, and a computing unit to encrypt the data. In this way, the chips are self-sufficient, offering all-in-one IoT capabilities, including security. State-of-the-art silicon-based complementary metal oxide semiconductors or CMOS, by contrast, are limited in terms of memory and computer integration due to their traditional von-Neumann computing architecture. Non-von-Neumann platforms such as field programmable gate arrays or FPGAs, however, lack sensing capabilities and require CMOS peripherals. The proposed three-terminal memtransistor technology — with the added feature of photosensitivity due to the material properties of MoS2 — offers a holistic solution that is critical to achieving integrated and energy- and area-efficient solutions.

An 8x8 crossbar array was fabricated for testing, the methods and results of which are published in Nature Communications. Using machine learning algorithms to study output patterns and predict input information, the research team found that these arrays should be safe from eavesdroppers, given finite resources and access to deep neural networks. That is, advanced machine codes couldn't decode encrypted information, and without prior knowledge of the information channels and decoding variables, it would be extremely difficult to do so.

In the near future, Das and the team plan to reach out to federal agencies and private corporations specializing in smart security in order to expand the scope of the research.

25. India witnessing growing interest in quantum computing: IBM

by Mini Tejaswi

https://www.thehindu.com/business/india-witnessing-growing-interest-in-quantum-computing-ibm/article65845348.ece

India has been witnessing growing interest in quantum computing, with students, developers, and academia actively participating. Consequently, the country is emerging as a talent hub for quantum computing, said Sandip Patel, MD, IBM India/South Asia region, in an interview.

What are the cardinal differences between quantum and classical computing?

Quantum computing is an exciting new technology that will shape our world of tomorrow by providing us with an edge and a myriad of possibilities. Quantum computing is a fundamentally different way of processing information compared to today's classical computing systems. While today's classical computers store information as binary 0 and 1 states, quantum computers draw on the fundamental laws of nature to carry out calculations using quantum bits. Unlike a bit that has to be a 0 or a 1, a qubit can be in a combination of states, which allows for exponentially larger calculations and gives them the potential to solve complex problems which even the most powerful classical supercomputers are not capable of.

How will quantum computing provide an edge over classical computing in terms of solving mankind's everyday challenges around life and work?

Quantum computers tap into the quantum mechanical phenomenon to manipulate information and are expected to shed light on processes of molecular and chemical interactions, address difficult optimisation problems, and boost the power of artificial intelligence. Advances like these could open the door to new scientific discoveries, life-saving drugs, and improvements in supply chains, logistics and the modelling of financial data. IBM today is actively working with major corporations and governments, to help advance their quantum roadmaps, and help grows their pool of quantum talent to make quantum computing practical for the benefit of science, industry and society.

What will be IBM India's contribution to Big Blue's global initiatives around quantum computing?

In India, we are witnessing a growing interest in quantum computing with active participation (amongst the highest) from students, developers, and academia in various initiatives like the IBM Quantum Challenge, IBM Quantum Summer School, Qiskit Challenge-India (Qiskit is an open-source software development kit built by IBM for the quantum developer community), and so on. We also have a growing community of Qiskit Advocates and IBM Quantum Ambassadors in India. Furthermore, we regularly organise India-focused programmes such as Qiskit India Week of Quantum, which celebrated women in quantum to kickstart their journeys in quantum, and was attended by almost 300 students. The Qiskit textbook is available in Tamil, Bengali and Hindi and was accessed more than 30,000 times by students in India in 2021 alone. We see India as a talent hub for quantum computing skills that is crucial for growing and maintaining such an interdisciplinary field.

Will you give us some details about IBM's collaboration with premier institutions in India to accelerate advanced training and research around quantum computing?

Academia plays an important role in building skills for any deep technology including quantum. Hence, last May, we announced our collaboration with leading educational institutions in India through the IBM Quantum Educators Programme. The faculty and students of these institutions will be able to access IBM Quantum systems, quantum learning resources and, quantum tools over IBM Cloud for educational purposes. This allows them to work on actual quantum computers and program them using the Qiskit open-source framework. In partnership with the Indian Institute of Technology - Madras, IBM conducted a course on Quantum Computing on the NPTEL platform last year, which had more than 10,000 participants. We are also collaborating with academia for joint research on quantum computing and recently, one of the research papers got accepted at a top Physics Conference.

At what stage is India in quantum computing, how long will it take to see commercialisation and where will it find mass applications?

India is poised to play a pivotal role in the quantum technology revolution globally. IBM is committed to helping India advance its quantum agenda by developing the talent and skills landscape and building an ecosystem with industry, business, academia and government. We are counting on the vibrant Indian talent and expertise to help solve some of the most pressing challenges. As per our quantum roadmap announced in 2021, IBM debuted its first 127-qubit processor. In 2022, IBM extended its quantum roadmap even further to clearly lay out how we will blaze a path towards frictionless quantum computing. This expanded roadmap includes our plans to build a 4,000+qubit processor by 2023, along with significant milestones to build an intelligent quantum software orchestration platform that will abstract away the noise and complexity of quantum machines, and allow large and complicated problems to be easily broken apart and solved across a network of quantum and classical systems. Once realised, this era of quantum-centric supercomputing will open up new, large, and powerful computational spaces for industries globally.

What is IBM's people strategy around quantum computing for Indian India?

In India, we have a strong team working across research, development, and consulting, working closely with academia, industry, and the public sector. Our team is working to support and accelerate India's national quantum mission and is participating in building a strong quantum ecosystem as that is crucial for succeeding. The team has been constantly growing to support the needs of the Indian ecosystem and is only expected to grow even further in the coming years as it supports more and more customers to take their quantum journey. We have quantum scientists and engineers around the world conducting fundamental research to improve the technology, as well as collaborating with our partners to advance toward practical applications with a quantum advantage for science and business. Quantum requires multidisciplinary skills and IBM has the best scientists and engineers working together to improve the technology and drive applications of importance to the industry.

26. Slimmed-down terminal transmits quantum keys from space

https://physicsworld.com/a/slimmed-down-terminal-transmits-quantum-keys-from-space/

Researchers in China have achieved a major milestone in space-to-ground quantum key distribution (QKD) by demonstrating a functional QKD terminal with half the mass of a previous system. After sending the new terminal into space to orbit the Earth aboard the Tiangong-2 space laboratory, scientists at Hefei National Laboratory and the University of Science and Technology of China (USTC) conducted a series of 19 experiments between 23 October 2018 and 13 February 2019, successfully transmitting quantum keys between the satellite and four stations on the ground on 15 separate days.

Like other QKD terminals, the device in this study relies on the quantum behaviour of light to create the kinds of encryption keys needed to protect data. "QKD employs the fundamental unit of light – single photons – to encode information between two distant users," explains Jian-Wei Pan, a physicist at USTC and a co-author of a paper on the research in Optica. "For example, the transmitter can randomly encode information on the polarization states of photons, such as horizontal, vertical, linear +45°, or linear −45°. At the receiver, similar polarization state decoding can be performed, and the raw keys can be obtained. After error correction and privacy amplification, the final secure keys can be extracted."

Future-proof security

The new slimmed-down QKD terminal is good news for users with high security requirements. Although traditional public-key cryptography is currently one of the best means of encryption, it relies on the fact that classical computers simply cannot solve certain problems in a reasonable amount of time. However, these intractable mathematical functions only work if the hacker is using a classical computer. As Pan points out, a quantum computer in the future could simply use Shor's algorithm to crack even the best current cryptography methods.

If quantum computers can break classical encryption, one possible solution would be to use quantum encryption instead, when applicable. "QKD provides an information-secure solution to the key exchange problem," says Pan. "The quantum no-cloning theorem dictates that an unknown quantum state cannot be cloned reliably. If the eavesdropper tries to eavesdrop in QKD, she unavoidably introduces disturbance to the quantum signals, which will then be detected by QKD users."

Paul Kwiat, a physicist at the University of Illinois at Urbana-Champaign, US, who was not involved in the research, adds that any attacks on QKD must be made at the time of transmission. "In this sense, QKD is sometimes described as 'future proof' – it doesn't matter what computation power some adversary develops 10 years from now (which would matter for public key cryptography); all that matters is the capabilities an eavesdropper has when the quantum key is initially distributed," says Kwiat, who leads the quantum communications division at Q-NEXT, a research consortium focused on quantum information challenges.

Daylight limitation

While previous QKD work has been conducted with a different device on the Micius satellite, in the latest study the researchers were able to reduce the terminal's mass by integrating the QKD payload with other systems such as control electronics, optics, and telescopes. This is a major step forward, but members of the Hefei–USTC team aren't finished. One challenge they mention in their paper is that they cannot currently run the terminal during the day. This is because scattering of sunlight creates background noise that is five to six orders of magnitude more than what is seen in experiments conducted at night. That said, Pan and his colleagues are working on technologies like wavelength optimization, spectral filtering, and spatial filtering to enable daylight QKD operation.

Pan states that the team has big plans, hopefully culminating in the creation of a global satellite-ground-integrated quantum network that can provide services to users worldwide. Following the success of this work, the team will begin constructing a quantum satellite constellation composed of several low-orbit satellites, a medium-to-high orbit satellite, and the ground-fibre QKD networks. "We think our work will contribute to an attractive area of research on how to construct the optimal satellite constellation," says Pan.

27. Current encryption and security will be null and void by 2030 at the latest

by Martyn Warwick

https://www.telecomtv.com/content/security/current-encryption-and-security-will-be-null-and-void-by-2030-at-the-latest-45317/

Even if you could afford it, you couldn't go out and buy a quantum computer today because they're a long way from being commercially available. However, that doesn't mean the machines don't exist – they do. It is known that there are such devices in the laboratories of commercial companies, in university research labs and military installations in various countries including the US and the UK, and the chances are that China, Russia and other countries also have them.

However, despite the intense international race to be the first to develop fully-functioning, full-sized quantum computers, currently, as far as practical applications are concerned, the experimental models are generally too small to outperform traditional electronic super-computers. That said, some have been developed to the point that they can be used to solve some heavy-duty tasks, such as integer factorisation.

In essence, integer factorisation this is the 'decomposition' of a composite number, which is a number can be made by multiplying other whole numbers. For example, 6 can be made from 2 x 3 and 15 can be made from 1, 3, 5 and 15, and thus is a composite number. When composite numbers become very large, no workable non-quantum integer factorisation algorithm has yet been found (although one might actually exist). The field of research is important because many cryptographic algorithms are based on the extreme difficulty of factorising large composite integers, and this has direct relevance and security of RSA public key encryption and the RSA digital signature.

Three years ago, a team of French researchers factored a 240-digit number that took 900 core-years of computing power to achieve, and from that experiment estimated that the factorisation of 1024-bit RSA modulus would take 500 times as long – in other words, 450,000 core years of computing. However, quantum computers can perform such calculations very quickly. A quantum computer utilising superposition, interference, and entanglement could crack and render instantly obsolete the ubiquitous RSA encryption algorithm in a matter of seconds. Soon, keeping information secret will become many orders of magnitude more difficult.

The "qubit" is the fundamental data processing element of a quantum computer and researchers are building machines with more and more of them whilst simultaneously developing error-correction methodologies that will enable the performance of longer and longer calculations. It's only a matter of time before all current encryption techniques will be rendered null and void. The general consensus within the industry is that this will happen by 2030 at the latest.

The search for post-quantum cryptography algorithms

The US National Institute of Standards and Technology NIST is leading the global search to discover standardisable post-quantum cryptography algorithms that will be both incredibly fast and completely reliable. It is hoped that at least two of them will be completed by 2024. The research is urgent right now because of the possibility (and even likelihood) that malign actors, many of them state-sponsored, are actively trying to harvest encrypted data that is uncrackable now, but will be able to be compromised when quantum computers are powerful enough - and that time will come soon. NIST says, "Nothing can be done to protect the confidentiality of encrypted material that was previously stored by an adversary." The organisation recommends that, for now, enterprises become "crypto agile" and work immediately to ensure their systems do not rely on just one particular encryption technology.

Simultaneously, another organisation, the Cybersecurity and Infrastructure Security Agency (CISA), is urging businesses to prepare to migrate to stronger cryptograph systems, adopt risk mitigation strategies and take an active part in the development of new standards. CISA is a US federal agency under the aegis of the Department of Homeland Security and it is urging businesses and organisations to follow its "post-quantum cryptography roadmap", at least until NIST publishes official guidelines and standards on the subject which will be completed towards the end of 2024.

CISA's post-quantum cryptography roadmap has seven main routes, the first being that the CEO and other C-level executives of any business should start to "increase their engagement with post-quantum standards developing organisations." Secondly, businesses and organisations should make an exhaustive inventory of the "most sensitive and critical datasets that will need to be secured for an extended amount of time." Thirdly, they should "conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future."

Simultaneously, "Cybersecurity officials within organisations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements." They should also identify where, and for what purpose, public key cryptography is being used and mark those systems as "quantum vulnerable." They must further prioritise one system over another for cryptographic transition based on the organisation's functions, goals, and needs. Finally, "using the inventory and prioritisation information, organisations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard."

It is very important advice, and as a new CISA statement stresses, "Do not wait until the quantum computers are in use by our adversaries to act. Early preparations will ensure a smooth migration to the post-quantum cryptography standard once it is available."

28. Intro to MongoDB's queryable encryption

by Matthew Tyson

https://www.csoonline.com/article/3671971/intro-to-mongodbs-queryable-encryption.html

MongoDB 6.0 introduces a preview feature that pulls off the quasi-magical feat of allowing encrypted data to be used as the target of searches, without ever transmitting the keys to the database.

Queryable encryption was the main attraction at MongoDB World 2022, for understandable reasons. It introduces a unique capability to reduce the attack surface for confidential data in several use cases. In particular, data remains encrypted at insert, storage, and query. Both queries and their responses are encrypted over the wire and randomized for resistance to frequency analysis.

The outcome of this is that applications can support use cases that require searching against classified data while never exposing it as plaintext in the data store infrastructure. Datastores that hold private information are a main target of hackers for obvious reasons. **MongoDB's encrypted fields means that this information is cryptographically secure at all times in the database, but still usable for searching.** In fact, the database does not hold the keys for decrypting the data at all. That means that even a complete breach of DB servers will not result in loss of private information.

Several prominent and sophisticated attack vectors are eliminated. For example:

- Unethical or hacked DB admin account.
- Accessing on-disk files.
- Accessing in-memory data.

This is something like hashing passwords. We hash passwords in the DB for the same reasons, so that it is impossible for a hacker or even the admin of the DB to view the password. The big difference of course is that hashing passwords is a one-way affair. You can verify if the password is correct, but that's it. There's no querying such a field and no way to recover the plaintext. Queryable encryption retains the ability to work with the field.

Another interesting characteristic of the system is that fields are encrypted in a randomized fashion, so the same value will output different ciphertext on different runs. This means the system is resistant to frequency analysis attacks as well. The system allows for a rigorous distinction between clients that have view privileges for the search results and those that don't, by controlling which clients have access to the keys.

For example, an application might store confidential information like a credit card number, alongside less sensitive information like username. A non-privileged client could see the username but not the credit card in a strict way, by not provisioning the client with the cryptographic keys. A client with access to the keys could see and use the credit card in searches, while keeping the card number encrypted at the steps of sending, searching, storing, and retrieving them.

Tradeoffs of queryable encryption

Of course all this comes at a cost. Specifically, there is a cost to space and time requirements for queries involving encrypted fields. (MongoDB guidance is around 2-3 times extra storage requirements for encrypted data, but that is expected to come down in the future).

Querying the encrypted data is handled by MongoDB incorporating metadata in the encrypted collections themselves, as well as separate collections with further metadata. These account for the increase in storage and time requirements when working with those data sets, along with the work of actual encryption and decryption.

Moreover, there is architectural complexity that must be supported in the form of a key management service (KMS) and the overhead of coding for employing it and the work of encryption and decryption itself.

How queryable encryption works

At the highest level, it looks like Figure 1.

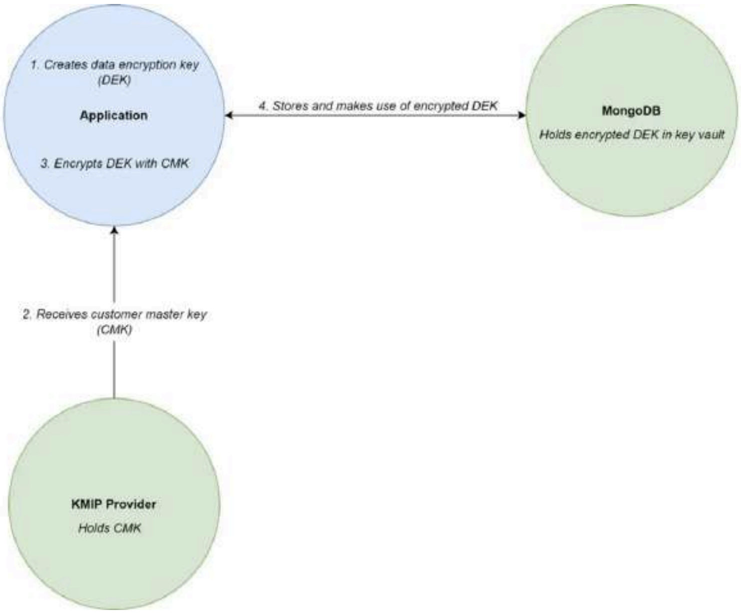

1. Creates data encryption key (DEK)
Application
3. Encrypts DEK with CMK
4. Stores and makes use of encrypted DEK
MongoDB
Holds encrypted DEK in key vault
2. Receives customer master key (CMK)
KMIP Provider
Holds CMK

Figure 1 illustrates that the system adds an architectural component: the KMS. The other change to the typical flow of events is that the data and queries are encrypted and decrypted via the MongoDB driver. The KMS provides the keys for this process.

Automatic and manual encryption

There are two basic modes for queryable encryption: automatic and manual. In automatic, the MongoDB driver itself handles encryption and decryption. In manual, the application developer does more hands-on work using the keys from the KMS.

Key types: customer master keys (CMK) and data encryption keys (DEK)

In the queryable encryption system there are two types of keys in play: the customer master keys (CMK) and the data encryption key (DEK). The DEK is the actual work key for encrypting the data. The CMK is used to encrypt the DEK. This provides extra security. The client application itself can make use of the DEK (and the data encrypted with it) only by first decrypting it with the CMK.

Therefore, even if the DEK is exposed in its encrypted form, it is useless to an attacker without access to the CMK. The architecture can be arranged such that the client application never holds the CMK itself, as described next with a key management service. The bottom line is that the dual key arrangement is an extra layer of security for your private keys.

Data encryption keys (DEK) are stored in an extra key vault collection as described below.

Key vaults

Data is encrypted with symmetric secret keys. Those keys belong to the app developer and are never sent to MongoDB. They are stored in a key vault. There are three basic scenarios for managing the keys, described below in ascending order of security.

1. **Local file key provider.**
   - Suitable only for development.
   - Keys are stored on local system alongside app
2. **KMIP (Key Management Interoperability Protocol) provider.**
   - Suitable for production, but less secure than using a KMS provider.
   - Customer master keys (CMK) are transmitted to client application
3. **Full KMS (Key Management Service) provider. Suitable for production**
   - Supported cloud KMS are: AWS, Azure and GCP
   - On-premises HSM (hardware security module) and KMS are supported
   - Only data encryption keys are transmitted to client application

Local key provider for development

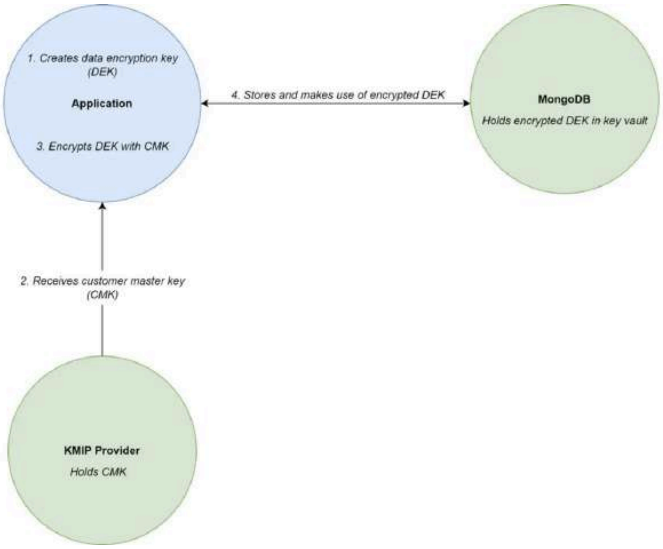
At development-time, the application developer can generate keys (say, with OpenSSL) and store them locally. Those keys are then used for encrypting and decrypting the information sent to and from the MongoDB instance. This is for development only because it introduces a major vulnerability to the secret keys that mitigates much of the advantages to queryable encryption.

KMIP provider

There are a number of KMIP implementations (including open source) and commercial services. In this scenario, the CMK is stored at the KMIP provider, and transmitted to the client app when the need for encrypting or decrypting the DEK for use arises. If the key vault collection is breached, the data remains safe. This arrangement is described in Figure 2.

KMS provider

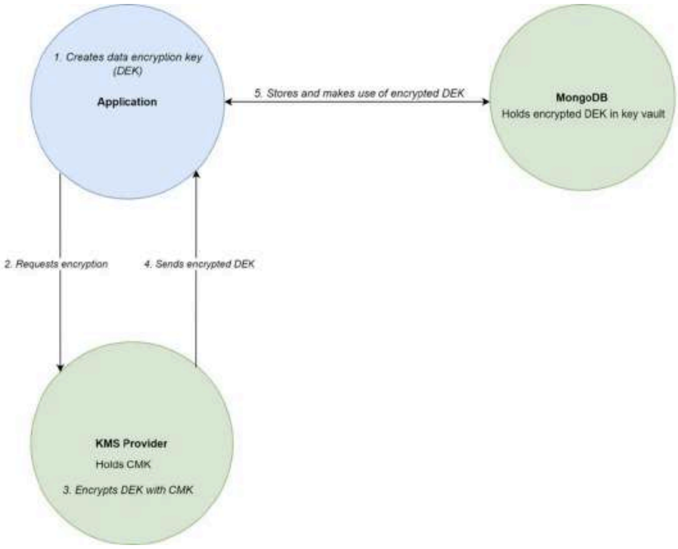
By using a KMS provider (like AWS, Azure or GCP) the customer master key is never exposed to the


1. Creates data encryption key (DEK)
Application
3. Encrypts DEK with CMK
4. Stores and makes use of encrypted DEK
MongoDB
Holds encrypted DEK in key vault
2. Receives customer master key (CMK)
KMIP Provider
Holds CMK

network or client app. Instead, the KMS provides the service of encrypting the DEK. The DEK itself is sent to the KMS, encrypted, and returned as cipher text, where it is then stored in a special key vault collection in MongoDB.

The stored DEK can then be retrieved and decrypted with the KMS in a similar fashion, again preventing exposure of the CMK itself. As in KMIP, if the key vault collection is breached, the data remains safe.

You can see this layout in Figure 3.


1. Creates data encryption key (DEK)
Application
5. Stores and makes use of encrypted DEK
MongoDB
Holds encrypted DEK in key vault
2. Requests encryption
4. Sends encrypted DEK
KMS Provider
Holds CMK
3. Encrypts DEK with CMK

Conclusion

Queryable encryption is a preview feature, and at the moment, only equality queries are supported. More query types like ranges are on the roadmap.

Although it requires extra setup, queryable encryption delivers a critical feature for use cases requiring search against confidential data that cannot be achieved in any other way. It is a compelling and distinctive capability.