PROTEGRITY

SHOR, GROVER, AND THE COMING STORM: QUANTUM COMPUTING'S RECKONING WITH MODERN CRYPTOGRAPHY

TABLE OF CONTENTS

01

Quantum Attack: A scenario

Buried inside Jingping mountain in the Liangshan Yi Autonomous Prefecture is the deepest and largest underground dark matter physics laboratory in the world. As an impressive tour-de-force, access to the lab is through a road drilled at the base of the mountain, allowing trucks to transport equipment of all sizes with ease. Most competing deep underground physics laboratories around the world use elevator shafts, and are, therefore, extremely restricted in their ability to move large objects, slowing down major equipment construction projects by months, if not years. Twenty years ago, the US National Science Foundation (NSF) reviewed and considered a proposal to construct a horizontal access deep underground laboratory in Washington State, but NSF backed out when the project ran into opposition from the local indigenous population.

At a depth of 1.5 miles, background interactions from cosmogenic events are minuscule, providing the world's best low noise environment. Only background from radioactivity in the surrounding rock needs consideration and can be tracked and corrected for with scintillating timing detectors.

Snaking between the large caverns and experimental halls is a labyrinth of roadways and tunnels serving the experiments and facilities for infrastructure support. Since fire is one of the primary hazards in underground laboratories, a repetitive spacing of fire-resistant unmarked metal-door enclaves exist along the roadways. However, behind one of these doors is a room that has nothing to do with fire protection.

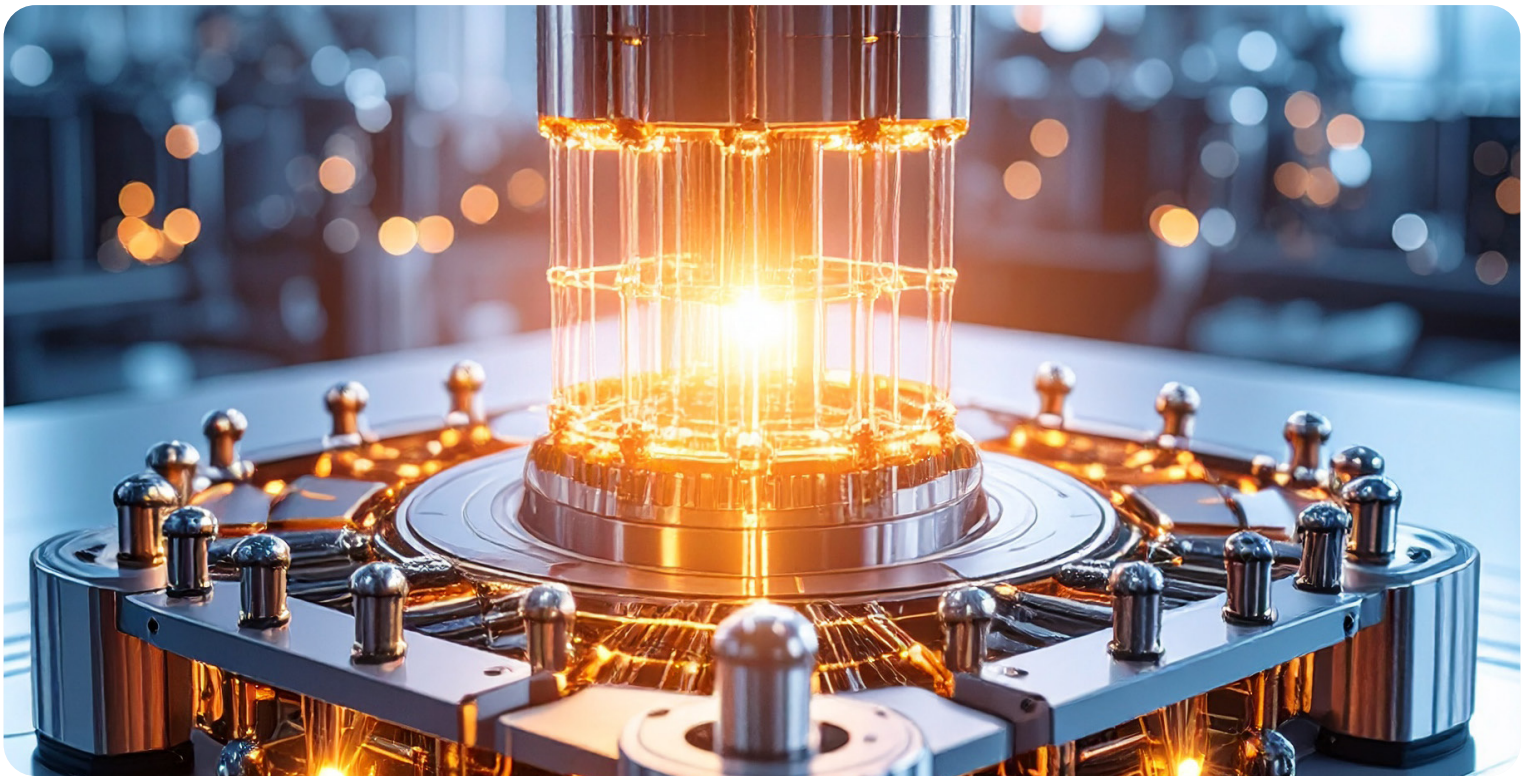
Here resides the world's largest and most powerful laser diode array, pumped by gallons of water cooling from the Jingping-II hydropower station and a firestorm of electrical power. Only Livermore's National Ignition Facility with its three-football field footprint competes in size and scale.

Tested, adapted and upgraded for decades, the laser system feeds light into a platform of hundreds of millions of neutral atom arrays excited to Rydberg states. These atoms become individual qubits, forming what is without question the world's first and most powerful quantum computer capable of implementing Shor's algorithm, to factor large numbers into its prime factors. Over ninety-nine percent of the atoms are used for quantum error corrections in response to the practically non-existent, but relevant backgrounds from the outside world.

Launched on Thanksgiving, the first calculation is directed squarely at the fictitious Satoshi Nakamoto. In a beautiful, choreographed dance, the atom arrays move rapidly in groups, changing and shifting positions, maintaining coherence, constantly monitored by neighboring error-correcting qubits, which are empowered to flip states and repair all whispers from the outside environment. Viewed from the top in slow motion, the rearrangements resemble a sophisticated, mesmerizing waltz. In reality, the speed of the calculation is breathtakingly fast and imperceptible to the human eye.

The computer runs autonomously for a month with a planned calculation completion date of Christmas Eve, at which point hellfire is brought down on Bitcoin as the computer busts through the private keys of an assembly of multiple Bitcoin owners, and funds are transferred circuitously to the Chinese government.

Of course, this is only a warning shot to the US, aimed next at encrypted nuclear weapons systems.



02

The Beast

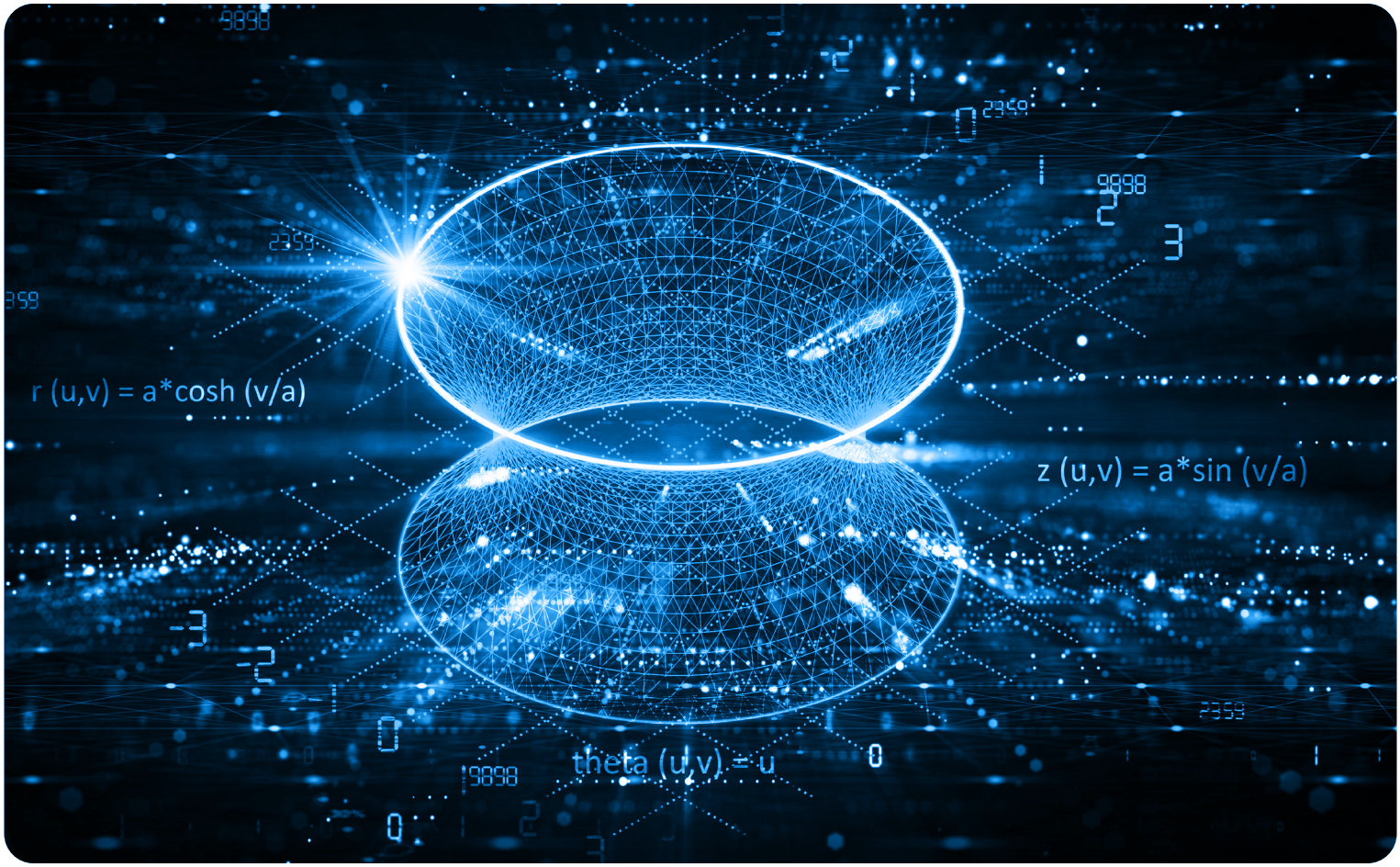
Asymmetric encryption—particularly RSA—is based on the multiplication of two large "hidden" prime numbers yielding a product that represents one piece of the public key. If one can factorize the public key, then the private key can be found (by a simple modular multiplicative inverse operation), and the encryption fails. Today's RSA encryption, used extensively for key and signature exchange, rely on RSA-2048 or RSA-4096, which are regarded as enormous and far outside the range of any conceivable conventional computer's ability to factorize the public key piece. Today, RSA is a gold standard.

The idea behind the largest threat to asymmetric encryption comes from a 1994 publication by Peter Shor in quantum computer science theory. Shor's algorithm is the beast and remains, thirty years later, the number one dark cloud danger to asymmetric encryption. Its search ability has an exponential nature that is astonishingly efficient.

In a nutshell, Shor's algorithm relies on the ability of quantum computers to find periods from Fourier transforms with extremely high efficiency, and this strength can be harnessed to rapidly converge in a search to factorize a large number constructed from the multiplication of two large prime numbers. Implementing the quantum version of a fast Fourier transform (FFT), the overhead time growth with number of bits is only quadratic, namely grows with n^2, versus the classical FFT which grows as $n2^n$. Although it may take a handful of runs of the quantum computer, the discovery of the period in the FFT results in a simple algebraic formula from which one finds the two prime numbers.

In practice, FFT requires finely spaced intervals for effective period searching, which demands a sufficient number of qubits to adequately explore the search space. In addition, the fidelity of the quantum computer must be kept intact, and large error correction schemes must be incorporated. Quantum computers that crack Shor's algorithm will require millions of qubits and error rates at the level of one part in a trillion. There are technical specifications that must be met to implement Shor's algorithm on a quantum computer.

When will this happen? Science and technology developments can sometimes take a century. Just estimate yourself when you think the world will have a nuclear fusion reactor as a regular, reliable energy source. Evaluating the status and danger in technology development for a quantum computer is a critical piece in the response and risk analysis for cryptographic protection.



03

Super Grover

What about protecting symmetric encryption? Symmetric encryption does not involve the multiplication of two large prime numbers and is, therefore, immune to attacks using Shor's algorithm. The primary threat comes from a brute force cycling through all possible character permutations over the length of the ciphertext. Today, AES-256 represents a gold standard and should withstand existing classical computer attacks on any reasonable time scale. Coming out of the quantum world, however, there is one annoyingly dangerous, but less catastrophic algorithmic threat. That is Grover's search algorithm.

In classical physics and the study of motion—apples falling from trees—we have Newton's laws. In quantum mechanics, Section 1, we have the Schrödinger equation. Quantum mechanics is all about precisely predicting probability distributions and how they change over time. The Schrödinger equation predicts how an object, called a wave function Ψ, varies over time. The probability is just the wavefunction squared, $|\Psi|^2$. This rule in quantum mechanics that you take your variable and square it to get an answer is fundamental, and this property of quantum mechanics is what gives Grover's algorithm its power.

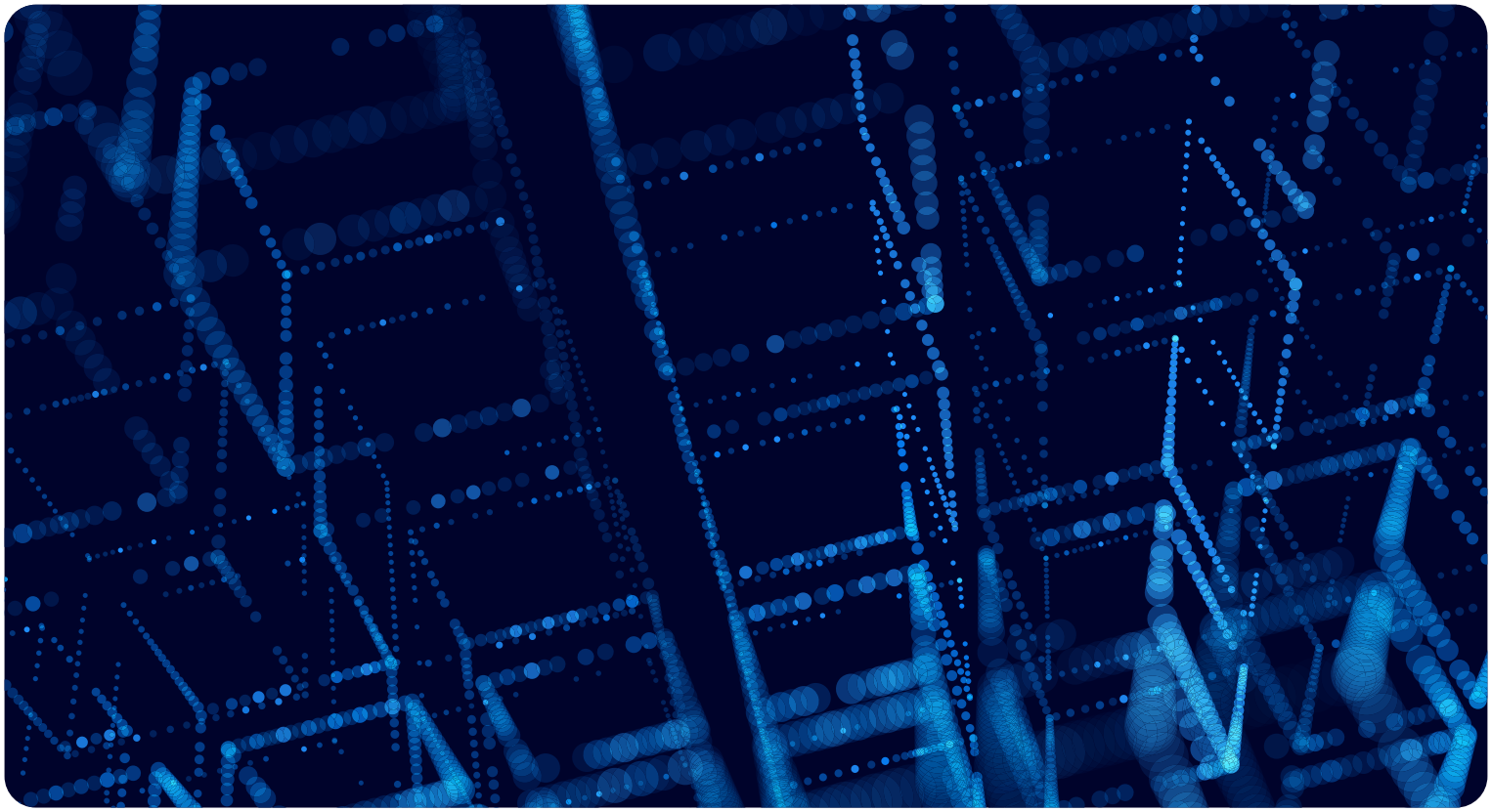
The insight from Grover's algorithm is that the brute force classical search can be mimicked by an equivalent brute force search over effectively the wavefunction Ψ. But, since everything is squared in quantum mechanics, the discovery space in that search improves by this square factor. If it takes 1 million search attempts to find something classically, it will only take 1000 attempts with a quantum computer, and this quadratic speedup persists to all numbers.

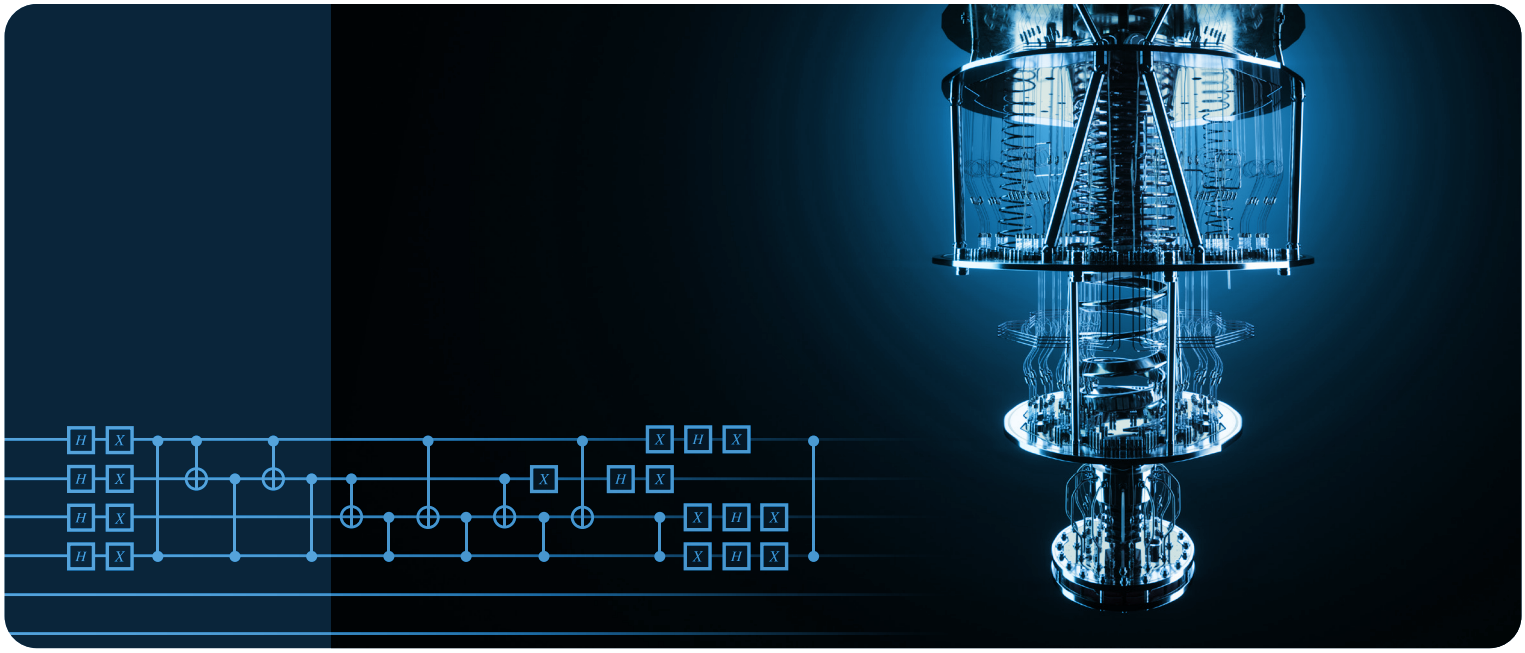
In practice, this means that to maintain equivalent security against a quantum search, the bit length of a ciphertext must be twice as long as what's required for a classical search. One million is 6 figures (base 10) and the square root of 1 million, which is 1000, is 3 figures (base 10). Today's AES-256 would need to be upgraded to AES-512 to have the same level of protection from a quantum attack using Grover's algorithm.

The circuit diagram for a Grover search is quite simple (see diagram on next page).

There is naturally a long list of caveats with respect to the dangers of a Grover attack, similar to a detailed analysis of the limitations of a Shor's attack. The technology and error rates need to be addressed.

Grover's algorithm, like Shor, was released thirty years ago in 1996. Both Grover and Shor's algorithms are well-established textbook examples of innovations from quantum computer theory. Surprisingly, there has been no new groundbreaking algorithmic innovations in the past three decades. Let's imagine, however, if there is a further investment in algorithmic developments and theoretical computer science training. Could a Super Grover algorithm be developed? Even another square root improvement in Grover's algorithm, based upon more sophisticated circuits, driven perhaps using AI, would have a sensational, transformative impact. Imagine a 1000 attempt quantum computer search mimicking a 1 trillion attempt classical computer search. Algorithmic developments in quantum computing are still in their infancy, but the interest, enthusiasm and training of workforce is rising rapidly.





04

Caesar Cipher

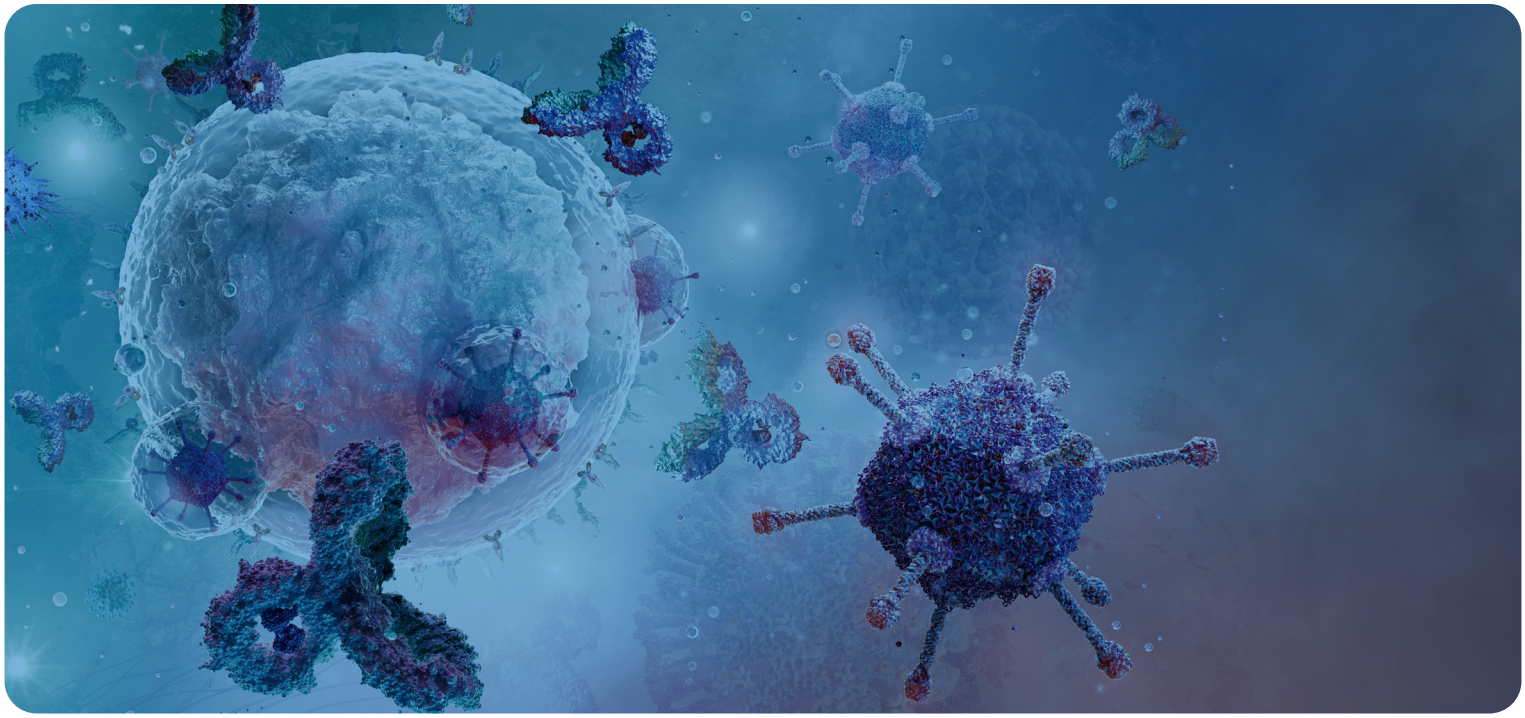
Where are we at present with quantum computers? Let's illustrate and discuss with one of the simplest encryption examples, the Caesar Cipher, which can be deciphered using Grover's algorithm implemented on Qiskit, IBM's quantum computing platform.

The Caesar cipher simply takes all the letters in the alphabet as a cyclic string (0-25) and then shifts the letters by a positive constant value K ("the key") and replaces the plaintext letter by the new ciphertext letter which differs in position in the alphabet by K. For example, if K=2, then A becomes C, B becomes D, ..., Y becomes A, and Z becomes B. Given some ciphertext, the goal is to find the value of K. This is an example of symmetric encryption and therefore within the world of quantum computers, one uses Grover's algorithm.

The application of even this incredibly trivial encryption code, developed in 100 B.C. and used by Julius Caesar for military communications, requires quite a sophisticated application of quantum computing to decrypt. The figure above shows a relatively simple circuit diagram of quantum gates needed to apply Grover's algorithm to find K.

More interestingly is the limitation today on quantum computing technical power. Firstly, IBM's publicly available quantum hardware cannot decipher the full 26 letter alphabet, since they do not have enough qubits to perform the calculation. Pretty humorous that the Caesar cipher is too sophisticated for today's publicly available quantum computers!

However, one can apply the calculation to a smaller alphabet, such as a hexadecimal string (0 to 15). Grover's search yields theoretically a result in $\pi/4\sqrt{N}$ iterations. For the hexadecimal case with 16 characters (0 to 15), N = 16 and number of iterations becomes just π, or effectively just 3 tries. Using ~30 qubits working on Qiskit, the probability of cracking the Caesar cipher code yielded a success of 91% for 2 attempts, 96% for 3 attempts and 58% for 4 attempts. The degradation in efficiency for a larger number of attempts is an interesting non-intuitive technical detail and results from overfitting the results. Non-intuition lies at the heart of quantum mechanics.

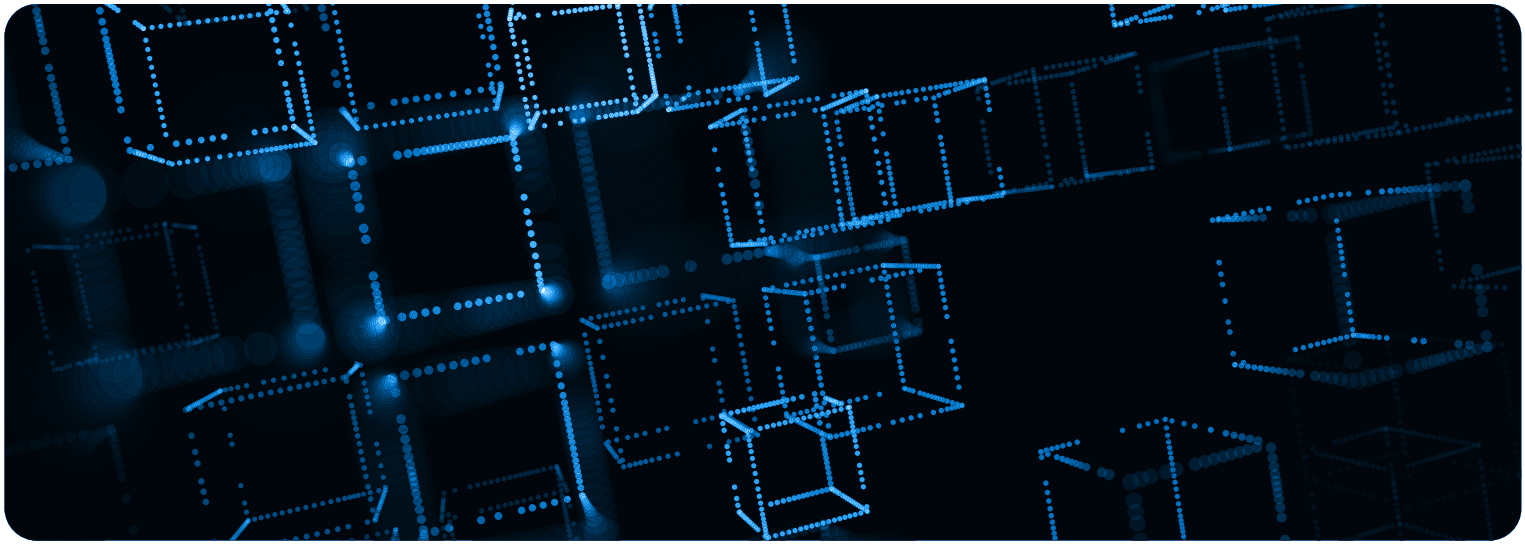


05

Bacteria versus Virus

Natural selection depends on three main characteristics, namely variation, inheritance and differential reproduction, all applied to large populations of organisms. (From the physicist point of view, this is an enormous ugly statistical mechanics problem.) In the never-ending battle for dominance at the cellular and sub-cellular scales, variations in the genetic code of viruses and bacteria continually change over time with often relatively small advantageous modifications becoming dominant and then spreading to the full population over generations. Think of all the different variants we learned about as the coronavirus was cruising through the world as a global pandemic. Viruses can enter and destroy the bacteria; however, genetically modified bacteria can develop resistances to the viruses, making them sterile. This same mechanism is behind the incredibly successful development of antibiotics and antibiotic resistance. This conflict is part of life and has likely been happening since the first bacteria appeared 3.5 billion years ago.

In the last decade, a critical biotech breakthrough—deeply entangled with the principles of natural selection—led to a Nobel Prize in Chemistry in 2020. It is called CRISPR. What is amazing about this technique, discovered almost by accident, was that nature has viruses, embedded in bacteria, called bacteriophages that can repair and modify the DNA inside the bacteria. The bacteria can be transformed into a factory that can selectively modify the DNA code, where the viruses become precise scissors that edit the DNA code. This hybrid model of bacteria and virus working in tandem is a transformational concept.



As a fun mental exercise, one can draw an analogy between this survival competition and the entire biosphere of cryptography and data protection. Everyone knows what a computer virus is, even though computers are not living objects. Bacteria are productive functioning organisms; so are computers, especially with AI. Although the scales are quite different, there are many of both.

Obviously, a quantum computer aimed to crunch out Shor's algorithm to unravel present-day asymmetric encryption is a super virus. Given such a beast or super virus, a roadmap and game plan need to be implemented, which at some level is being actively pursued by the NIST analyses of post quantum cryptography (PQC). Many open questions remain. Can classical computers, redirected to PQC repel or slow down a quantum attack? Can they even detect such an occurrence? Does one need a quantum computer with offensive and defensive capability to remain competitive? Is there a bacteriophage solution in which some hybrid of quantum technology with classical computers offers enough safety to diminish this threat?

How does Protegrity play into this issue?

The heart and soul today of much of Protegrity protection is the Protegrity Vaultless Tokenization (PVT). This is a wonderfully successful and powerful local product in which data is protected wherever it resides, moving or static. There are no mathematical relationships between the plaintext and ciphertext. The tokens, by themselves, are useless to a hacker. PVT depends on static lookup tables and multiple rounds of chaining, resulting in an non-traceable diffusion that transports the ciphertext far from its origin. Protegrity estimates that the PVT process is more secure than AES-256, which is unbreakable in any reasonable estimate of brute force decryption using classical computers.

A Grover attack on PVT would be repelled by an upgrade in string length, similar to moving from AES-256 to AES-512. God forbid that a kept-secret Super Grover attack is developed which degrades the security back to AES-128, which would no longer be secure. If quantum computer code did advance in the next couple of decades to more dangerous codes, the hope is that there might be enough advanced warning. This is the realm where PQC codes would be useful to encircle as added protection. PVT is easily upgradable if one needs to move to a larger key, as would be done if one migrates to AES-512. Even converting SLT 3x2 to SLT 6x2 may be adequate.

Protegrity's strength, namely tokenization, is also its weakness. Protegrity today only addresses symmetric encryption. Like most of the world of communication, Protegrity relies upon RSA for the secure transfer of data. Store now/ decrypt later is a particularly commonly discussed threat. See Section 9 for future discussion.

Cryptocurrency with its heavy reliance on public key exchange is particularly susceptible to an attack from the super virus.

06

Errors, Erros, Erors

Quantum computers are like humans, filled with errors and obeying no rational logic. To build a computer that will successfully apply Shor's algorithm is comparable in scale to building the perfect human. The biggest challenge is correcting errors, coming from the interaction of the qubits with the outside world. What one wants are completely isolated qubits, interacting strongly with each other through entanglement, and absolutely no other influence from the outside environment. Purely nature. No nurture. The maximum error rate for the successful application of Shor's algorithm against today's asymmetric encryption codes is estimated to be on the order of 10^{-11} to 10^{-12}. Today's error rates are on the order of 10^{-3}, which already incorporate non-trivial, even sophisticated, error correction schemes.

Moreover, one logical qubit may require a thousand (or thousands or more) qubits just to correct for environmental errors. As one might imagine, optimization is a massive undertaking. At the next level of detail, one must account for the number of logical qubits, the depth of the circuit, and the overhead from quantum error correction qubits, both serial and parallel overhead. Critical technical inputs to estimations of the danger include the cycle time of the qubits, often estimated to be on the order of 100 ns, changes in the error rates and improvements in quantum codes that yield higher throughput rates.

As a rule of thumb, over the past years, there appears to be an inverse Moore's law for the decrease in error rates for quantum computers. Every two years, the error rate decreases by a factor of two. If this rate is maintained, it would take on the order of 60 years to develop the Beast. Of course, the uncertainty on this assumed "Moore's law" rate is large and even a small change in the base value can swing the results to substantially different time scale estimates.

Research in quantum algorithms and quantum circuits is still very much in its infancy. Any paradigm change that reduces the load on the quantum computer specifications could have a transformative effect on unraveling asymmetric encryption. Tracking research developments is a critical piece of protection against quantum computers.

Other quantum technology advances may circumvent some of the challenges ahead. A program to develop more complicated qubits, called qudits, that correspond to a larger quantum spin state could potentially simplify the quantum algorithms and accomplish the same goal as Shor with less algorithmic steps. This likely relies on more experimental control over a more complicated system, but it might arrive sooner.

07

Immortality

A nuclear war could end the human species and life on earth as we know it. The worldwide fires that would be created by a nuclear war between the US and Russia, for example, would send so much soot into the air that light from the sun would be blocked, and the result would be freezing temperatures and worldwide mass starvation. The world population is approximately 8 billion, and it has been estimated that 5 billion deaths would result from starvation due to a nuclear war between the US and Russia. This could happen at any moment, especially with a mistake.

In response to this horrific dilemma and the dangers of nuclear war, a Doomsday Clock was created in 1947 by the Bulletin of Atomic Scientists. Set initially at 7 minutes to midnight, the clock is adjusted annually by a committee of eminent scientists aimed to reflect changes in the risk of nuclear war over time. Midnight represents nuclear war and seconds away from midnight represents the relative danger of nuclear war, tracked annually. Today, the clock is the closest that it has ever been to midnight, set at 89 seconds to midnight. This is not regarded as a silly exercise by the scientific community that created the nuclear bomb or the disarmament community, but, instead, is an attempt to raise awareness.

Real fear exists that a quantum computer will take down classical computer security systems someday, wreaking havoc on the financial community as well as many others. Evaluating that risk is a serious component of the dangers of quantum computing. If quantum computers do not exist, by definition, a computer security system is absolutely quantum proof. One could debate whether a decrypting quantum computer danger could be as soon as 5 years away or 100 years away or anywhere in between. For the ~5 years scenario, the assumption is that some country has advanced the technology significantly beyond what is known publicly in a hidden quantum computing Manhattan Project, coupled with giant steps in quantum simulation codes that make Shor's algorithm negligibly weak in comparison. For the 100 years or more scenario, one considers cases where scientific and technical research have fallen short. Ask yourself honestly on what timescale do you think fusion energy, which began with the detonation of the hydrogen bomb in 1952, really will become available as a controllable energy source. Probably not within a 100 years of its conception.

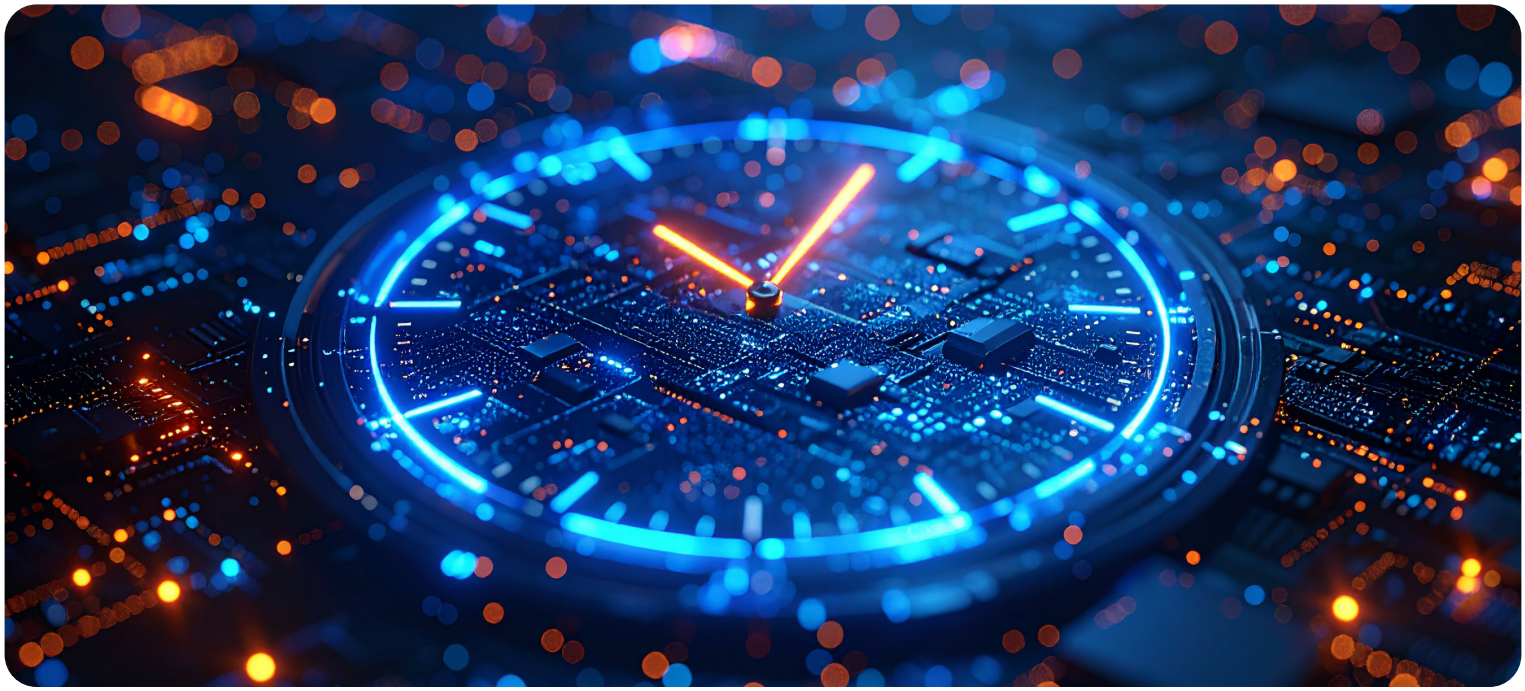
Getting some handle on the probability of the danger of quantum computers coming to life, as the technology advances, is a serious piece of the puzzle. A quantum Doomsday clock would provide some community focus on evaluating the time-dependent evolution of danger.

A final comment on process is worthwhile.

When the Federal Reserve decides to change interest rates, the process involves a committee of experts to evaluate the impact on the economy. This is not a mathematical algorithm; it involves a deep dive into many technical details and confidential discussions. The robustness of the process has been one of the gold standards for the US economy for decades.

When the nuclear Doomsday clock is adjusted annually, it similarly involves a decision by a committee of nuclear disarmament experts. The direct impact of the proximal approach of the second hand to midnight is difficult to measure, but the clock is well known worldwide and at least a constant public reminder to the nuclear weapons states and the nuclear disarmament communities.

Interest rates and clocks provide single-valued focus. See Section 9 for further discussion on this topic.



08

Achilles Heel

In all the doom and gloom, there is a ray of hope, since the quantum computers are, indeed, not perfect, even if they are built with an error rate that can deliver on Shor's algorithm, the Beast. Today's RSA-2048 would be vulnerable to attack. However, there are numerous other difficult search algorithms where there is no evidence that quantum computers would perform better than classical computers. Restated, these algorithms are identified to take exponential timescales to solve classically and there is no solution today in which a quantum computer would do any better.

A simple example is the traveling salesperson problem. If a salesman starts at his home and visits numerous customer locations and then return to his home at the end of the trip, what is the optimal order in which he visits the customers to minimize the transit time? This conceptually simple problem is a complicated "exponential" calculation as the number of customers increases. Today, there is no evidence that a quantum computer could solve this problem better than a classical computer.

Turned around, if a quantum computer cannot solve a problem better than a classical computer, then that problem becomes an Achilles heel for quantum computers. Efforts focused on converting encryption and tokenization using math problems where having a quantum computer is not an advantage provides protection for classical computers. The entire Post Quantum Cryptography competition that NIST has been orchestrating since the start of the Trump 1 administration shepherds in these quantum resistant algorithms.

One particularly promising classical algorithm that is believed to be quantum resistant and rising high in the NIST competition is lattice-based encryption. Without doing a deep dive, the algorithm relies on the difficulty of solving hard problems in high-dimensional lattice structures, which are grids of discrete points in a multi-dimensional space. This gives access to vectors with angles and lengths in higher than one-dimension, complicating significantly any search algorithm that tries to uncover hidden variables. The challenge to using lattice-based encryption, or any of the other quantum resistant options, will be the impact on latency and conversion to the existing world of encryption. How tolerant will the community be to the added protection, burdens and expense in light of whatever assessed threat comes from a near or far future quantum computer attack?

09

Now What?

In academia, whenever a faculty committee finishes its study, the usual recommendation is to set up another committee to study further. The result is an infinite do loop with no crash protection. Tenure does not help the problem.

For a White Paper, the usual recommendation naturally is to produce a Roadmap. What is the roadmap for this purported White Paper? What should Protegrity do about Quantum? Quantum has continued to rise in importance over the past decade, primarily due to its threat to public key encryption and, in fact, any asymmetric encryption system now in place. The fear exists and mapping some sort of response and timeline is needed.

Key questions are:

- Is the threat real and on what timescale?
- What can one do in the next decade to protect systems?
- What education and capacity-building are required to respond to this new threat?
- Are there emergent relevant quantum technologies, short of building a quantum computer?
- Does everyone eventually have to build or buy a quantum computer?

PROTEGRITY'S RESPONSE TO THESE QUESTIONS CAN BE SUMMARIZED HERE AND REQUIRE A ROADMAP AND MORE STUDY:

- Fast incorporation of quantum resistant codes within near term versions (next year or two) into the company product. Start with NIST-approved or near-approved codes. Assessing the impact on latency will be critical. At first, these should have on/off capabilities, since the short-term risk of quantum computers is small, if not negligible. This is priority one.

- To build quantum capacity into the company requires education, which is best accomplished by creating an R&D arm. Target first smaller quantum technologies that could become products. (One example may be a BB84 quantum key distributor for data transport.) Evaluate quantum simulations for cryptography. Carefully cost out the creation of an R&D arm. This may take a year.

- Creation of a Quantum Doomsday Clock to track technical developments and evaluate dangers and risks. This could be created cheaply within months timescale. Target goals should be submissions to Black Hat and Def Con conference in the summer 2026. This project should build some reality-based expertise to the quantum computer threat and be led by young, committed researchers in quantum computing. It would be invaluable to develop data, metrics and graphs, comparable to the importance of Moore's Law, to track progress in quantum technology developments.

- Learn how to run quantum calculations on publicly available platforms as some small fractional effort for the company programmers. Perhaps create a Protegrity Quantum Computing course. This can be accomplished cheaply, if done in house. This could be created within a year timescale, if not faster.

- Work on educating customers regarding risks and benefits of quantum. Start now.

- Consider purchasing a quantum computer as a backburner idea in the not infinite future. Track quantum computer products as they emerge.

- Transform this last Section 9 into a publicly-available mini Roadmap for Protegrity's quantum activities, plans and investments for the next few years.

PROTEGRITY.COM