

00 00 32 42

DAYS

HOURS

MINUTES

SECONDS

The Big Clock

Established decryption technologies, the brains and hearts of current-era cryptography, are up against an ominous triple witching hour: gradual obsolescence, quantum computing, and alarming corporate complacency. Time is running out for the old order. Will the world make needed changes while there's still time?



THEON
TECHNOLOGY®

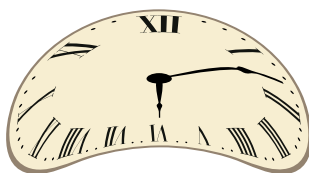
Scott Bledsoe, Chief Executive Officer
Brian Anderson, Chief Marketing Officer
Joseph Mulvihill, Senior Technical Business Analyst
Theon Technology



Abstract

Standard cryptographic algorithms employed for decades face an ominous ticking clock in the form of massive quantum computing advances. Breakthrough-level quantum processing power holds the destabilizing potential to upend everyday digital security by rendering our most common go-to ciphers next to useless. Quantum developments therefore have potential to cripple secure, timely transmission of sensitive digital data. Influential government agencies such as NIST recognize the potential threat and campaign to advance the state of the cryptographic arts with new, more sophisticated technology standards. Too often, however, private

interests display unfortunate complacency toward information security – or the stubborn, problematic conviction that old, established solutions will remain viable despite the alarming threat landscape. A breakthrough cryptographic technology is available, however, that mitigates the essential vulnerabilities in last-generation algorithms; it is inspired by the OTP or one-time pad cipher, the only solution of its kind deemed perfect and unbreakable. The clock is ticking for the old order, but it is possible to reduce risk exposure – and perhaps dodge disaster – by adopting an evolved approach to humankind's oldest challenge: keeping secrets.



CONTENTS

Introduction.....	4
Tick, Tick, Tick.....	8
Through the Looking Glass.....	10
Guerrillas Hit the NIST.....	15
A Quantum of Complacency.....	19
The Only Known Clock-Stopper.....	22
Conclusion: The Big Clock.....	25

Introduction

Someday, the force that rocked the long-established, taken-for-granted cryptographic order and compelled the invention of a new one may be remembered simply as 九章.

九章

Image Credit: Hansen Zhong

The Big Clock © 2022 Theon Technology

Westerners who keep tabs on the cryptography threat landscape know 九章 as Jiuzhang.

Jiuzhang is among the most celebrated citizens of Hefei, Anhui province, China, landlocked about midway between Beijing and Hong Kong. Anhui province is home to the picturesque Yangtze and Han River basins and also the University of Science and Technology of China, where Jiuzhang is a lifelong resident.

But Jiuzhang does not go out for sports or stroll the banks of the Yangtze on weekends. Jiuzhang is a computer: the first photonic quantum computer to claim quantum supremacy – that is, the capability to not only perform tasks far faster than traditional, “classical” computers, but do things classical computers simply cannot.

One such thing is the breaking down of complex factorizations. Success means a fast pass to unraveling factor-based cryptographic algorithms.

In 2020, Jiuzhang performed an operation in 200 seconds that would likely have taken 2018’s fastest

classical supercomputer, the Sunway TaihuLight, 2.5 billion years. (The task concerned Gaussian boson sampling, but let’s not get sidetracked.¹) In 2021 a precocious sibling, Jiuzhang-2, completed a task in one millisecond for which a conventional computer would likely require 30 trillion years. Jiuzhang-2 clocked a new top speed for a quantum processor.²

By running up such numbers, 九章 stabbed the old cryptographic order in the heart.

Today’s entrenched cryptography paradigms are rooted in ideas and ciphers more than a century old. Virtually every aspect of everyday life has evolved, from what we eat and wear to how we communicate and exchange data, but not our basic intellectual approach to keeping secrets. We have mostly transferred pre-digital models and techniques to the computer age.

The Vernam Cipher, the revolutionary cryptographic aid devised during World War I, has evident echoes in today’s standard cryptographic technologies: the everyday algorithmic locks plus complex digital keys that make it possible for you to buy pizza and plane

tickets via your smartphone.

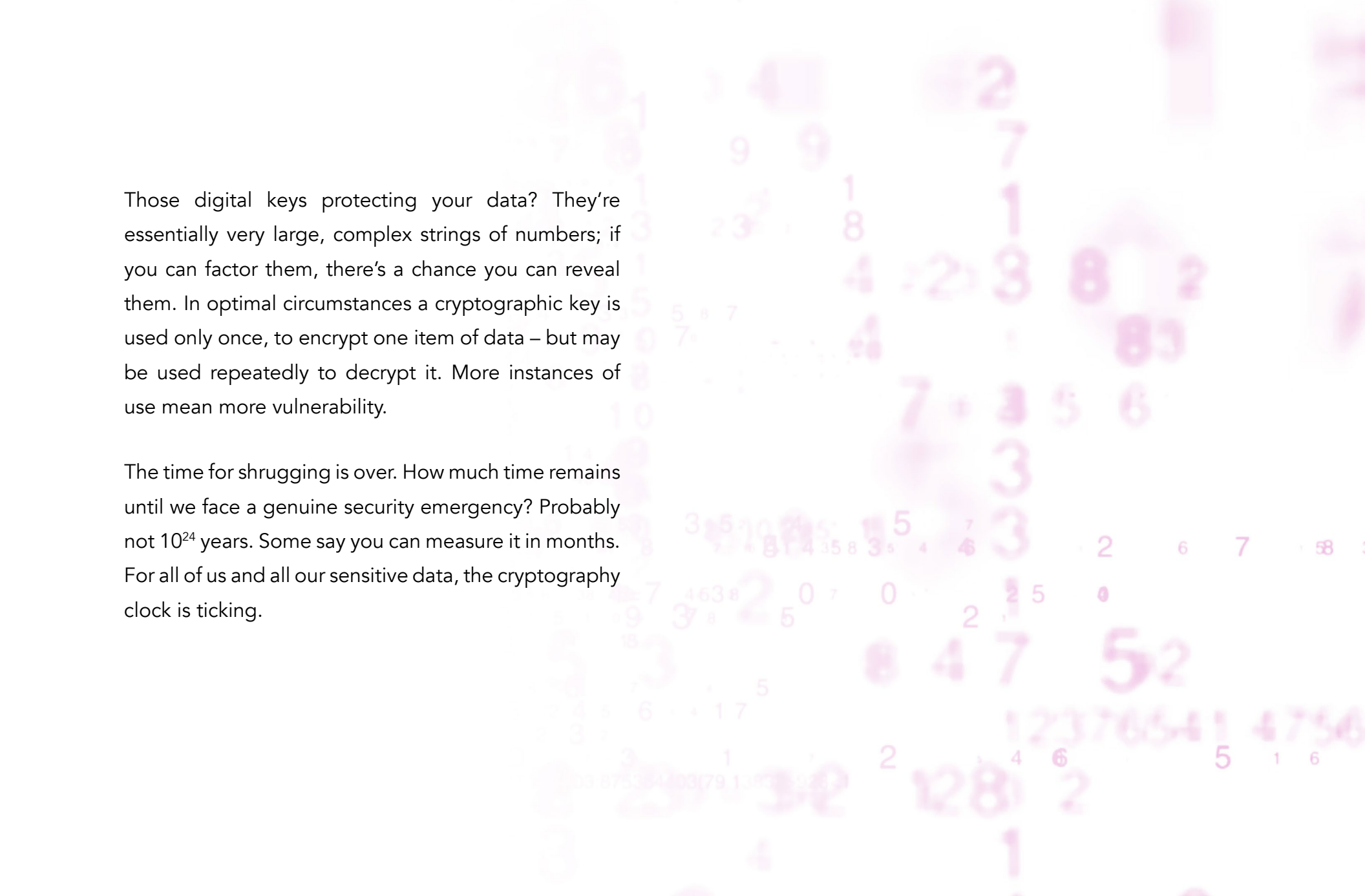
So far, status quo encryption and decryption standards afford us fairly good digital security. While the Vernam Cipher-inspired OTP, or one-time pad, remains the only cryptographic model deemed absolutely impregnable, other, lesser ciphers toil away embedded in essential digital systems. A breezy term has emerged for them: “Computational security,” which denotes imperfect but acceptable security. Pretty good, it seems, passes for good enough – especially since true OTP cryptography is challenging to deploy at enterprise scale.

Defenders of the pretty good status quo are fond of repeating statistics indicating that cracking a typical critical, go-to cipher in use today would take a computer 10^{24} years, or some other unimaginable length of time. Therefore, they conclude with a confident grin, computational security is all the shield most of us will ever need.

Quantum computing begs to differ.

The aging systems we use for data encryption are at increasing risk. They’re threatened by recent advances in higher mathematics and ever-more-resourceful cyber pirates. But the big X factor is the steady advance of quantum computing: Jiuzhang, Jiuzhang-2, and all their up-and-coming silicon cousins worldwide. The state of the quantum arts moves forward with neck-snapping speed and constitutes something of a superpower arms race, with China, Russia, and the United States angling for high ground. Another prodigy of USTC Hefei, called Zuchongzhi 2.1, quickly supplanted Jiuzhang-2 as the world’s most powerful quantum computer, but IBM aims to regain the pole position with its Quantum Condor.³

The act of routine data decryption, which you likely trigger many times a day, knowingly or not, while relying on venerable old technologies, is particularly vulnerable to unfriendly quantum deciphering efforts.



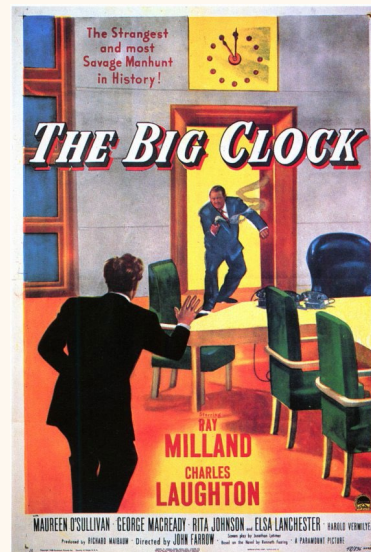
Those digital keys protecting your data? They're essentially very large, complex strings of numbers; if you can factor them, there's a chance you can reveal them. In optimal circumstances a cryptographic key is used only once, to encrypt one item of data – but may be used repeatedly to decrypt it. More instances of use mean more vulnerability.

The time for shrugging is over. How much time remains until we face a genuine security emergency? Probably not 10^{24} years. Some say you can measure it in months. For all of us and all our sensitive data, the cryptography clock is ticking.

Tick, Tick, Tick



In the 1948 noir classic *The Big Clock*, a crime magazine editor is desperate to crack a murder case stacked against him as time runs out and walls close in. Circumstances argue Ray Milland's character, George Stroud, killed his boss' mistress. Stroud knows his boss (a scheming Charles Laughton) did the deed, but the boss is framing *him*. Stroud, however, can't prove it. He's assigned to lead a high-profile investigative dragnet to find the murderer – knowing all clues point to himself – while a looming clock in the office lobby ticks off his remaining minutes of freedom.



we have only so much secure time remaining. The suspense is in the question: **What will we do to change our circumstances?**

So far, not enough. The security and stability of the digital order are threatened by onrushing quantum computing power, which stands to ramp data vulnerability way up into

the red zone. Shor's algorithm provided a white-board proof way back in 1994. Now here comes real-world hardware to precipitate a genuine, not just a white-board, emergency.

Does Stroud get the goods on his evil boss in the last reel? Let's not spoil a suspenseful movie. The point is, the palpable, existential dread that permeates *The Big Clock*, an ominous inkling of circumstances stacked against us and time expiring, is present in cryptography today. Or should be.

Shockingly, with a few noble exceptions – digital Paul Reveres, riding to attract attention to this looming threat – the general response to date from most quarters has been an inertial shrug, more or less. Assertions of faith in status quo “computational security.” The pretty good kind.

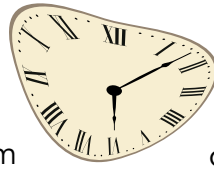
There's a big clock ticking for us, too – all digital citizens, institutional and individual, who take data security for granted. Innocent as George Stroud we may be, but innocence is beside the point. It looks like

The technologies at the core of most current, load-bearing cryptographic solutions haven't changed appreciably in decades.



Through the Looking Glass

You need not be a scientist with a capital S to appreciate quantum computing's potential to infiltrate decryption events and destabilize day-to-day data security. Here's a thirty-second primer on a couple of key points.



You may have read about quantum physics, quantum mechanics, or quantum field theory, which investigate the fundamental ways matter and energy behave in the physical universe. Albert Einstein famously called quantum mechanics “spooky action,” because of observed behaviors that seemed to defy conventions of human understanding.⁴ Concrete rules of physics once taken for granted can wilt when you dig into quantum mechanics.

When it comes to blowing up cherished expectations, the difference between traditional and quantum computing is not so different.

Traditional or classical computers process every form of data into ones and zeroes. It’s a dead-simple binary vocabulary; a standard, regular computing bit must be either 1 or 0, and even the fastest, hot-rod classical computers need a tiny iota of time to flip back and forth between 1s and 0s in order to process information. Supercomputers such as those used by military and intelligence agencies process oceans of data and expose hidden connections. AI and machine learning programs perform impressive deductive feats

on these machines. But they’re all flipping between 1s and 0s – just applying more horsepower to the task than the chip in your smart coffee maker, which runs on the very same binary principle.

Superconducting quantum machines are fundamentally different. They’re not limited by the processing hurdles – all that flipping – inherent in classical computing. For this discussion, the key thing to know is that in quantum computing, bits are out, qubits are in. A qubit is a quantum bit, which can be *both 1 and 0 simultaneously*. No more flipping back and forth; no more time allotment for same.

Spooky action indeed. Quantum information sciences and technologies, QIST for short, have endless capacity to confuse – how can the same bit represent two different values at once? – but also surprise and impress. China’s Zuchongzhi 2.1 has an approximately 60-qubit processor, good enough to rate as the world’s most powerful quantum system. IBM’s Quantum Condor, said to be ready for assignment in 2023, is rumored to be capable of processing 1,121 qubits.⁵



All this power can deliver highly useful things. Volkswagen is said to be working on a quantum computing platform able to predict traffic jams 45 minutes before they occur. (Your dashboard navigation display can only tell you about them once they exist.) Quantum computing can theoretically debug millions of lines of software code in seconds and give us breakthrough health care treatments. “Without quantum computers, new DNA sequencing data, the learning of the specific activities of the folded conformations of proteins, and the search for new drugs by docking algorithms, are being held back from full clinical application,” says a New York State Department of Health researcher, Donald Parsons.⁶

But not all quantum breakthroughs are embrace-worthy.

“This promises to speed up computing immensely, enabling assaults on henceforth uncrackable problems like decrypting currently unbreakable codes, pushing AI and machine learning to new heights,” say researcher Thomas Corbett and technology strategist P.W. Singer.⁷

As an example, take RSA, the most widely used asymmetric encryption algorithm – asymmetric meaning it uses a public key for encryption, a private key for decryption. It was first described in theoretical form in the late 1970s, developed for general use by a company founded in 1982, and patented in 1983. (The initials R,S, and A refer to the algorithm’s inventors: Ron Rivest, Adi Shamir, and Leonard Adleman.) You probably don’t drive a 40-year-old car or watch a 40-year-old TV, but asymmetric algorithms like RSA keep the secure world spinning despite being of similar vintage or even older.

What makes RSA secure – up to now, anyway – is the idea that the monster-length numerical keys it employs are very hard to factor. You multiply two big prime numbers, the logic goes, and the result is an even bigger, virtually impenetrable one. A number that would take even a supercomputers an inordinate, impractical length of time to factor. The whole security proposition comes down to faith in the notion that factorizing very large integers – a prelude to decryption – is too computationally difficult.⁸

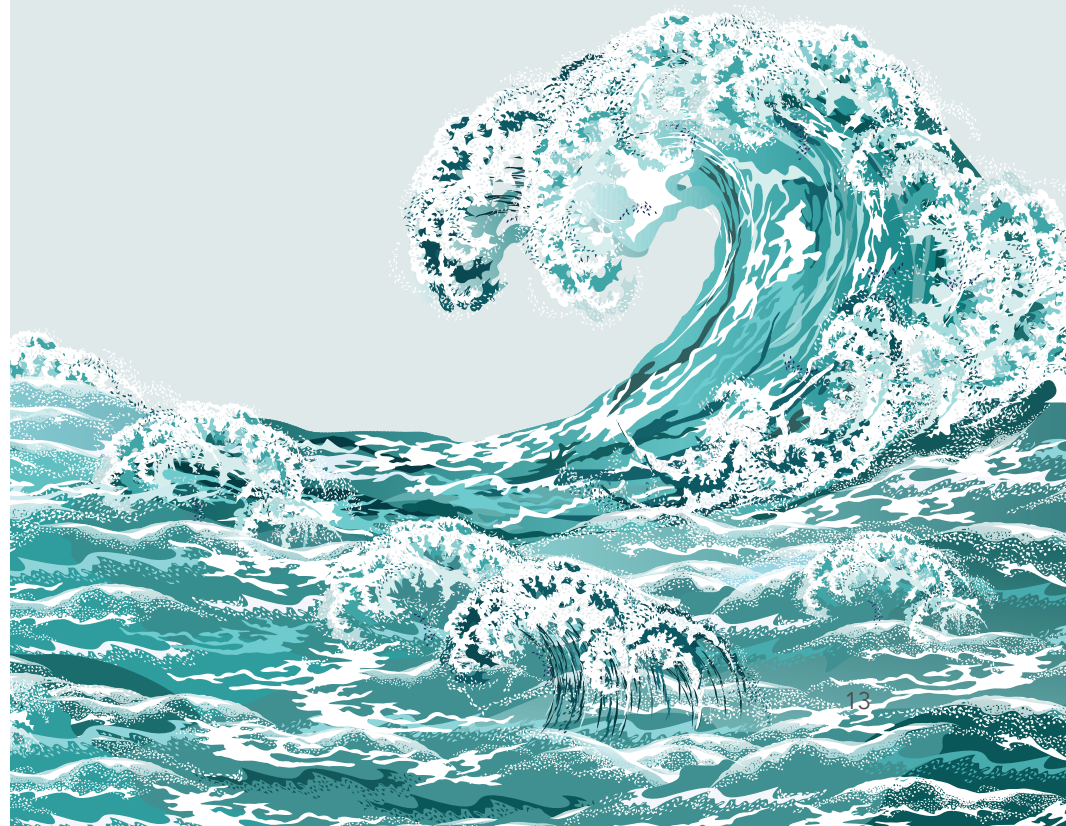
Well, 九章 has entered the chat. And in this new light, there are many weak keys at work in the world. Even AES (for Advanced Encryption Standard), the block cipher technology that probably inspires the most confidence today, has been a standard solution now for two long decades. When it comes to future vulnerabilities, nobody has a crystal ball.

"Quantum computing... poses significant risks to the economic and national security of the United States," stated a solemn National Security Memorandum to US civilian and military leadership in May 2022.

"Most notably, 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."⁹

A few researchers are even more unequivocal. "What was once believed unbreakable doesn't exist anymore," Terra Quantum lead research physicist Valerii Vinokur has declared.¹⁰

It is human nature, perhaps, to put off coming to grips with grave threats until they are wreaking havoc, unmissably, right there in your front yard. We've all watched blithe Florida beachgoers surfing on TV with a hurricane just over the horizon as wiser souls evacuate inland. Can't see the storm? Can't see the problem. Let's catch another wave.



We see some of that what-me-worry? attitude in the cryptography debate today. Google any set of terms encompassing quantum computing and data security. You'll find no end of conventional wisdom assuring you any possible emergency lurks in the far-off future if it's a possibility at all. It's the same sort of wisdom that murmurs mantras about computers still requiring 10^{24} years to break a foundational cipher, so relax.

All right; let's suppose they're right. Suppose the quantum threat really is way over the horizon – dismissible today, even. There are still compelling reasons to quit surfing.

Threats to conventional algorithmic decryption are clear, present, and rising even without a quantum computer. We've seen extraordinary strides in higher mathematics since the turn of the century; one cryptographic key sold as recently as 2020 was cracked "instantly" by a German researcher using a factorization technique from the 1600s.¹¹ AI and machine learning are becoming more crafty, capable attack tools, too.

Human error is not going out of style; a majority of data loss incidents can be traced to mistakes committed by personnel. They range from getting suckered into clicking on phishing links to sloppy IT hygiene, like storing decryption keys in proximity to the data they protect or even reusing them. Better security would protect us from ourselves.

There's also the "harvest now, decrypt later" threat – the practice by data thieves of stealing sensitive material even though it eludes decryption by unauthorized eyes right now. The data can be stored in anticipation of quantum deciphering capabilities becoming accessible in the future. This scenario is sometimes waved off by dedicated surfers. They argue that such data will be stale and useless by the time it's deciphered – you'll probably have different credit card numbers in the 2030s. But this is a little too blithe. You'll still have the same Social Security number. Even stale data has some utility.

A more prudent course of action would be to migrate to an encryption protocol that defies quantum attacks and other threats. **The Big Clock is ticking.**

Guerrillas Hit the **NIST**



NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. For years it has struggled gamely to promote better, safer standards and practices in the digital security sphere. NIST has invested a formidable sum of taxpayer dollars in this effort, going back to the days when quantum dangers to cryptography were more hypothetical and seemed far less proximate.

“People have to understand the threat that quantum computers can pose to cryptography,” says Dustin Moody, who leads the post-quantum cryptography project at NIST. “We need to have new algorithms to replace the ones that are vulnerable, and the first step is to standardize them.”¹²

But NIST has not had an easy go of things.

One noble recent NIST initiative is a competition to support development of the post-RSA, more quantum-resistant standard algorithms favored by Moody. The Post-Quantum Cryptography Standardization Project was launched in 2016; private-sector innovators were

invited to submit their best shots; a short list of winners would be considered for elevation as new approved standards. 69 entries materialized for round one, and the field was winnowed again and again until a sort of Final Four emerged in mid-2022.

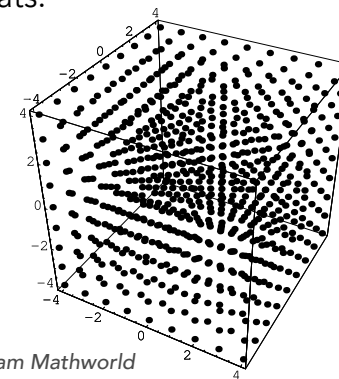
Getting to this point required NIST to fight a three-front battle. There was – still is – stubborn affection out there for the old, increasingly obsolescent cryptography paradigms, particularly from economy-minded private interests.

There’s the Big Clock problem. The standardization process won’t be complete until 2024. With eye-popping QIST innovations emerging every few months, eight years is a long gestation period for standards meant to neutralize quantum threats. And that’s not counting time for rollout, adoption, and implementation. Moody at NIST estimates it will take 10 to 15 years for private companies to implement eventual NIST standards at meaningful scale. By that time, the threat landscape will no doubt have evolved to a state we can only guess at today.¹³

And third, there's a technology problem: a striking number of promising aspirants blew up on the pad, even in the late innings, after exhaustive evaluating and winnowing. Not always because of quantum challenges, either. One prominent casualty was Rainbow, a digital signature algorithm featuring a secret key known only to the user. A scientist affiliated with IBM Research called Ward Beullens cracked Rainbow open, guerrilla-style, in less than a weekend armed only with a standard-issue laptop. Years of effort notwithstanding, Rainbow was benched.¹⁴ Similar ignominy befell SIKE (short for Supersingular Isogenic Key Encapsulation), which weathered many rounds of scrutiny to be named an alternate to the Final Four. Not long thereafter, SIKE was laid tragically low in almost casual fashion, not by Jiuzhang-2 or anything close but a lowly single-core PC. The brutal takedown hack took one quick hour.¹⁵

"The newly uncovered weakness is clearly a major blow to SIKE," lamented its co-inventor David Jao, a professor at the University of Waterloo. "The attack is really unexpected."¹⁶ But aren't they all?

The NIST competition's Final Four survivors included one algorithm for general encryption, CRYSTALS-Kyber, and three for use in digital signatures: CRYSTALS-Dilithium, FALCON, and SPHINCS+. CRYSTALS-Kyber is cast as a rough category replacement for RSA: an asymmetric key solution designed to create trustworthy connections over public, unsanitized, untrustworthy networks. The big departure versus RSA (you can skip to the next page if you wish): with RSA, as we said earlier, the cryptographic keys are factors, vulnerable to being revealed by QIST power in sinister hands. The mathematical basis of CRYSTALS-Kyber is an abstract, multi-dimensional grid or maze called a structured lattice, and the keys are vectors through the maze. As complicated as it sounds, and hopefully frustrating to quantum threats.

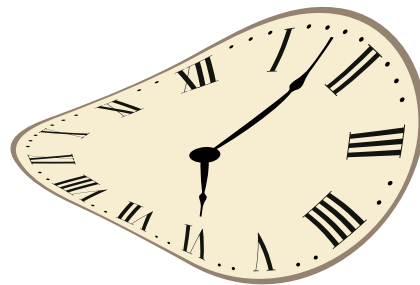



Cubic Lattice
Image Credit: Wolfram Mathworld

It is one thing, of course, to admire a shiny new technology proposition on the showroom floor, quite another to buy it and get stuck in rush-hour traffic. “Assessing security is usually a cat-and-mouse game,” says Artur Ekert, University of Oxford quantum physics professor. “Lattice-based cryptography is very elegant from a mathematical perspective, but assessing its security is really hard... a more detailed security analysis is needed.”¹⁷

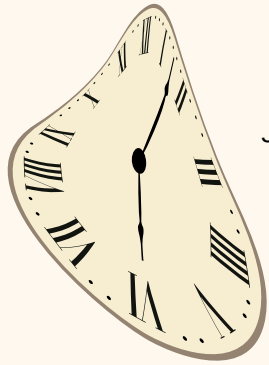
And despite all this honorable effort by NIST and its many innovators, suppose these new-generation algorithms, not due to hit the street until mid-decade, are actually crackable today by faster, hotter, QIST hardware still under wraps – computers perhaps strictly controlled by nation-states? The U.S. Air Force doesn’t show off every new warplane test-flown at Area 51; why would security-minded governments reveal the extent of their true quantum capabilities?

The United States government is of course working both ends of the quantum street – defense and offense. While NIST sounds virtuous alarms about quantum security threats, and the White House rolls out an elaborate timeline for migrating federal agencies away from cryptographic solutions not rated quantum-resistant,¹⁸ the Pentagon in 2021 requisitioned \$688 million for QIST research and technology. U.S. policymakers are building QIST partnerships with other countries and accelerating research under the National Quantum Initiative Act.¹⁹ In other words, one arm makes the Big Clock for conventional cryptography tick faster – while another labors to beat it.





A Quantum of Complacency



Just because governments demonstrate alarm about quantum threats does not mean private interests toe the same line. Urgent, focused action is spotty at best despite the NIST example. A lack of commitment and conviction at the corporate level has sadly been a consistent feature of the modern digital security era. (Remember, “pretty good” security still has legions of enthusiasts.)

Osterman Research surveyed the “maturity level” of cloud security organizations in North America and found, to universal consternation, that 84% rated themselves at merely entry-level cloud security capabilities – and 80% reported they lack a dedicated security team responsible for protecting cloud resources from threats.²⁰

A mid-2022 PwC survey of business executives found the top risk on their minds wasn’t inflation or talent retention, but cybersecurity. Good news. And yet only about 49% said they were increasing their investment in cybersecurity, and among small businesses there was even less concern: only 5% named cybersecurity

their biggest risk, even though the US Small Business Administration says 25% of small businesses are hit by cyberattacks, and fully half the victims don’t survive.²¹

NIST has coped with such obstinacy for years. In 2016 NIST advised organizations to wean themselves away from SMS-centric two-factor authentication, or 2FA – the quick-expiring numerical verification codes you’re sent so you can access your brokerage statement. They’re easy to compromise and vulnerable to interception bots. We’ve known it for years. Yet if anything, more private businesses than ever are proudly rolling out 2FA, proclaiming their undying commitment to protecting your data.

When it comes to information security, corporate complacency is evident everywhere, and presents a threat as troubling in its way as the external, malevolent kind.

Why? Obviously bottom-line financial factors play a role. Despite spiraling threats, SOCs (security operations centers) and CISOs are eternally urged to do more with less. There is a global security

talent deficit which can fuel organizational chaos: in mid-2022 there were more than 700,000 unfilled cybersecurity jobs in the United States alone – and 3.5 million vacancies worldwide, a situation not expected to improve through mid-decade.²² Stress and burnout help drive high churn rates in the security ranks.

Residual trauma from bad security solution deployments in days gone by may also help encourage corporate avoidance. Maybe decision makers tire of being constantly exhorted to transform their businesses, again and again, to avoid some new half-apparent menace. And in some quarters, there's the persistent, faith-based sentiment that tried-and-true security strategies are still mostly OK even though history tells us deprecation, in the fullness of time, spares no technology.

Maybe, they might think, it's even less risky to stick with a decades-old workhorse than to undergo a paradigm shift. Not the case, but we get that. Maybe – and there's no polite way to say this – some decision makers get brainwashed.

In this new, uncertain era, however, there is one way to beat the clock – and the quite real menace – and protect encrypted information. It should hold special appeal for decision makers who think they've spent too much, bet too wildly, or suffered too greatly in the past from security implementations that went south.



The Only Known Clock-Stopper



The need is acute for a new encryption solution that surmounts the vulnerabilities of past-generation RSA-class algorithms and anticipates the next-generation, quantum-era threat landscape.

A new approach must resist not only QIST assaults, but new forms of non-quantum threats, including advances in higher mathematics. And it has to be deployable at scale, economically and efficiently, across the gigantic, diverse, rapidly expanding digital information realm. No advance, technological or otherwise, can have impact if it's unaffordable or inefficient.

The best basis for better cryptography is the so-called one-time pad mentioned earlier: OTP for short. OTP remains an unbeatable standard, still widely regarded as the only perfect cipher. Properly executed, with single-use keys that are genuinely random, unique, and secret, OTP neutralizes generalized quantum threats and enables uncrackable encryption. It is not only the best way to beat the Big Clock and preserve digital security in the coming quantum era; it is the only known way.

Yet for all its natural virtues, pure OTP has proven challenging to adopt at scale. It requires issuance and transmission of a cryptographic key equal in size to the data file it's protecting in transit. That means double the file size in motion, and OTP keys consume additional storage space and processing power. It takes more effort and energy to deploy and support traditional OTP – yet another argument for sticking with other approaches that are “good enough” for present day, but of uncertain efficacy in future.

Now, however, comes a way to leverage the natural advantages of OTP and frustrate quantum attacks while mitigating OTP's historical disadvantages.

Theon Technology employs an advanced mathematical equation to propagate truly random, high-entropy cryptographic keys at scale. A unique key is issued for every item of data in your care. Theon has innovated a breakthrough key creation and storage solution that addresses the biggest issues with OTP: unwieldy key size. This approach to OTP key generation means very large OTP keys need not be transmitted from

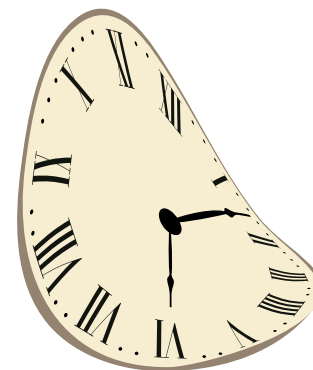
one locale to another. It's provided within a symmetric solution – using private keys, not public ones – that leverages proprietary software. That separates the Theon solution from ciphers vulnerable to factorization such as RSA.

And in stark contrast to all those algorithms vying to improve on the last generation but proving painfully vulnerable to hack attacks, OTP is the only encryption technique ever deemed “perfect” by the father of modern information theory, Claude Shannon.

Of course organizations weary of challenges to “transform your business” might be loath to dynamite their security infrastructure. Doing so is expensive, and transformation doesn't always pay off; it can create techno-quagmires of half-operational solutions which increase cost and risk in other ways. One of the few points in favor of inertia is, it works some of the time – as long as the threat coast is clear. And inaction is cheaper until disaster hits (at which point it becomes very expensive indeed).

But the OTP-inspired quantum-resistant encryption solution from Theon can be layered over existing deployments. It is not mandatory to tear out an established security infrastructure. The Theon solution can be added as an additional prophylactic measure.

In a computing environment where IBM's Quantum Condor and its 1,121 qubits of power are imminent and nobody knows exactly how the quantum threat landscape is about to evolve or who has the upper hand, a next-generation encryption approach based on the only “perfect” cipher may be an insurance policy worth considering.





00 00 42 32

DAYS HOURS MINUTES SECONDS

Conclusion: The Big Clock

The clock is ticking down the years, perhaps months, to “Q-day” – the day when quantum computing performance is readily available – to perform noble tasks, yes, but perhaps also break the internet by upending the old cryptographic order with acts of aggression.

Through the lens of digital security, brute QIST force in malign hands threatens more than your retirement fund, local electric grid, or traffic light controls. Look at the contest among superpowers to achieve superiority in a quantum arms race – a race that has already yielded demonstrations of literally incomprehensible problem-solving power. Such power is inherently destabilizing and threatening, but it cannot be wished away. And while governments don't want grade-A QIST in malevolent hands, there is no foolproof way to sequester it. By its very nature, quantum computing is harder to control than the weapons of mass destruction that terrorized the 20th century. Yet rendering our dominant incumbent digital security technologies ineffective would certainly qualify as a kind of mass destruction in itself.

What is the most rational response to such uncertainty? **It is to do what far too many decision makers currently hesitate to do: act preemptively to secure what is yours.**

Throughout the history of the digital era, most failures and penalties have been suffered by those who dawdled in the face of change, failed to spot trends, or waited to be engulfed by crisis.

There are few if any penalties for reading the future and beating the clock.

We'll conclude with a spoiler. At the climax of *The Big Clock*, George Stroud does indeed connect the dots, prove his innocence, and save himself while the cops and the press chase red herrings and swallow false narratives. In cryptography, too, every organization has the power to protect itself. To defy inertia and acquire better shields against proximate dangers.

If only there were 10^{24} years to act, as proponents of the status quo suggest. But with each passing month, the quantum threat to cryptography grows, complacency looks more and more like an inadequate strategy, and that sound you hear is the ticking of our own Big Clock, ever louder.





Contact Theon Technology

info@theontechnology.com

Or visit

theontechnology.com

ENDNOTES

- 1 Philip Ball, "Physicists in China Challenge Google's 'Quantum Advantage,'" Nature, 3 December 2020.
<https://www.nature.com/articles/d41586-020-03434-7>
- 2 Thomas Corbett and Peter W. Singer, "China May Have Just Taken the Lead in the Quantum Computing Race," Defense One, 14 April 2022. <https://www.defenseone.com/ideas/2022/04/china-may-have-just-taken-lead-quantum-computing-race/365707/>
- 3 Zhanna Malekos Smith, "Make Haste Slowly for Quantum," CSIS (Center for Strategic and International Studies), 11 February 2022. <https://www.csis.org/analysis/make-haste-slowly-quantum>
- 4 Davide Castelvecchi, "How Spooky is Quantum Physics? The Answer Could Be Incalculable," Nature.com, 16 January 2020. <https://www.nature.com/articles/d41586-020-00120-6>
- 5 Jay Gambetta, "Expanding the IBM Quantum Roadmap to Anticipate the Future of Quantum-Centric Supercomputing," IBM Research newsroom, 10 May 2022.
<https://research.ibm.com/blog/ibm-quantum-roadmap-2025>
- 6 IEEE Standards Association, "Quantum Computing Will Change Everything, and Sooner Than You Expect," Futurism, 12 October 2017. <https://futurism.com/quantum-computing-change-sooner-than-expect>
- 7 Thomas Corbett and Peter W. Singer, "China May Have Just Taken the Lead in the Quantum Computing Race," Defense One, 14 April 2022. <https://www.defenseone.com/ideas/2022/04/china-may-have-just-taken-lead-quantum-computing-race/365707/>
- 8 Michael Cobb, "RSA algorithm (Rivest-Shamir-Adleman)," TechTarget.com.
<https://www.techtarget.com/searchsecurity/definition/RSA>

- 9 “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,” WhiteHouse.gov, 4 May 2022.
<https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>
- 10 Ryan Gallagher, “Swiss Firm Terra Quantum Uncovers Vulnerabilities That Imperil Encryption,” Business Standard, 8 February 2021. https://www.business-standard.com/article/technology/swiss-firm-terra-quantum-uncovers-vulnerabilities-that-imperils-encryption-121020800131_1.html
- 11 Dan Goodin, “Researcher Uses 379-Year-Old Algorithm to Crack Crypto Keys Found in the Wild,” Ars Technica, 14 March 2022. <https://arstechnica.com/information-technology/2022/03/researcher-uses-600-year-old-algorithm-to-crack-crypto-keys-found-in-the-wild/>
- 12 Amit Katwala, “Will These Algorithms Save You From Quantum Threats?” Wired.com, 8 July 2022.
<https://www.wired.com/story/quantum-proof-encryption-is-here-but-theres-a-catch>
- 13 Katwala, Wired.com, 8 July 2022.
- 14 Raul Limon, “Using Just a Laptop, an Encryption Code Designed to Prevent a Quantum Computer Attack Was Cracked in Just 53 Hours,” El Pais, 23 March 2022.
<https://english.elpais.com/science-tech/2022-03-24/using-just-a-laptop-an-encryption-code-designed-to-prevent-a-quantum-computer-attack-was-cracked-in-just-53-hours.html>
- 15 Lucas Ropek, “Supposedly Quantum-Proof Encryption Cracked by Basic-Ass PC,” Gizmodo, 2 August 2022. <https://gizmodo.com/quantum-encryption-algorithm-nist-broken-single-core-pc-1849360898>

- 16 Dan Goodin, "Post-Quantum Encryption Contender is Taken Out by Single-Core PC in 1 Hour," Ars Technica, 2 August 2022. <https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/>
- 17 Katwala, Wired.com, 8 July 2022.
- 18 "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," WhiteHouse.gov, 4 May 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>
- 19 Zhanna Malekos Smith, "Make Haste Slowly for Quantum," CSIS (Center for Strategic and International Studies), 11 February 2022. <https://www.csis.org/analysis/make-haste-slowly-quantum>
- 20 "Osterman Research Survey Finds 84% of Companies Have Only Rudimentary Capabilities for Securing Their Cloud Infrastructure," BusinessWire, 4 August 2022. <https://apnews.com/press-release/business-wire/technology-middle-east-tel-aviv-c2a6eb17d0844e71a7c484e3697bac70>
- 21 Andy Medici, "Move Over Inflation and Hiring. Executives Say This is Their Biggest Risk," The Business Journals / bizjournals.com, 23 August 2022. <https://www.bizjournals.com/bizjournals/news/2022/08/23/cybersecurity-pwc-talent-hiring-cyber.html>
- 22 Sydney Lake, "Companies are Desperate for Cybersecurity Workers—More Than 700K Positions Need to Be Filled," Fortune.com, 30 June 2022. <https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/>