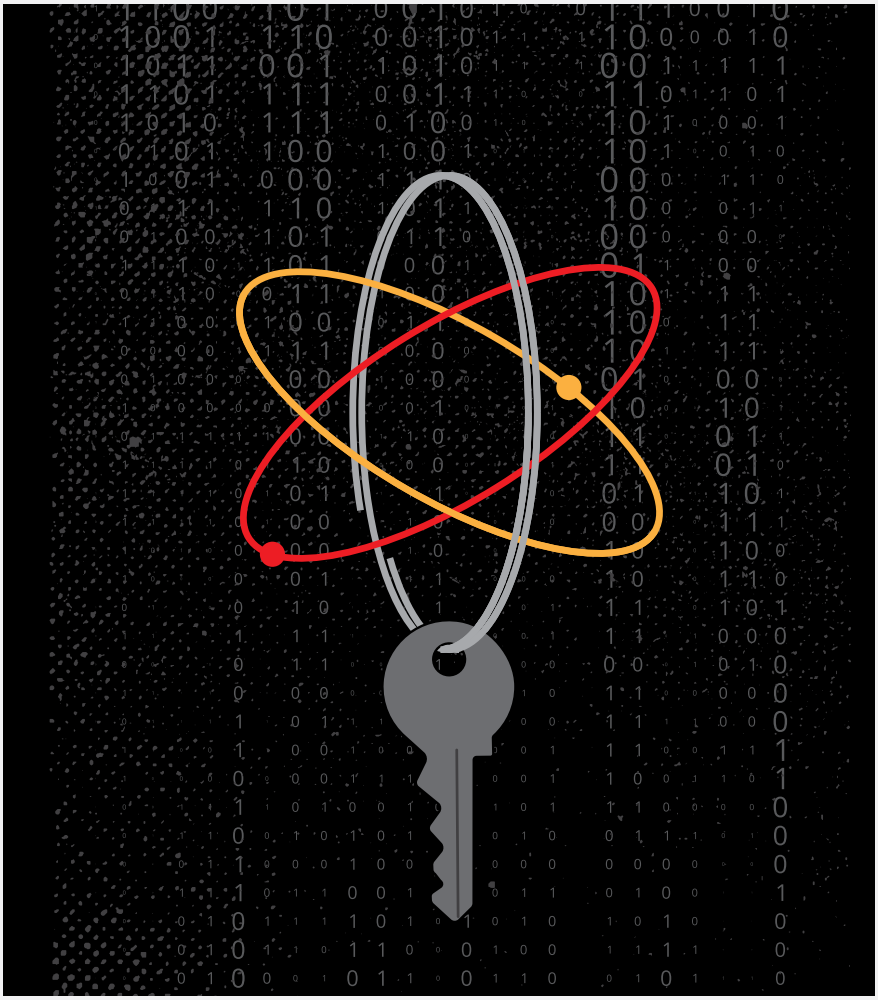

Is your organization prepared for Post-Quantum Cryptography?

Cryptography Is Facing a Quantum Apocalypse

By Andrew Hardin

Data encryption, a foundational element of information security, relies on the principles of cryptography to secure underlying information using a mathematic algorithm and a "secret key." Safety comes from the fact that it is prohibitively time-consuming[1] to decrypt the data without possessing an encrypted file's secret key, and the secret keys themselves are equally difficult for attackers to reproduce. But the advent of quantum computing has changed the underlying assumptions of cryptography, and with sufficiently sized quantum computers, encryption that would have previously taken trillions of years to break could fall in the span of a typical workday.[1]

Today's quantum computers lack the power needed to quickly defeat the most commonly used traditional encryption schemes, and it will still be several years[2] before this changes. But when quantum computers do achieve the needed scale, all our traditional cryptographic defenses will become susceptible, an event that is often referred to as the "quantum apocalypse." Worse, even encrypted data stolen today and stored will be susceptible to decryption by quantum computers in the future.[3] This "harvest now, decrypt later" scheme means that, even now, traditional encryption is not enough to secure data from the coming quantum threat.

The good news is that there are steps you can take now to reduce your risk: namely, implementing Post-Quantum Cryptography (PQC).[4] But PQC is not right for all organizations yet, and implementing it today will not help protect traditionally encrypted data that is stolen before PQC is in place. So, what should you do to protect yourself from the quantum apocalypse? This article will cover some of the factors that should be taken into account when determining the appropriate strategy for your organization, as well as actions you can take to mitigate risk *today*.

Even encrypted data stolen today and stored will be susceptible to decryption by quantum computers in the future.

The State of PQC Today

In July 2022, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) selected four PQC algorithms to be used when replacing traditional, susceptible cryptographic systems: CRYSTALS-Kyber for data encryption, and the remaining three for digital signatures. Fundamentally, these algorithms attempt to do for quantum computing what classical cryptography does for traditional computers—make the time cost prohibitive when attempting to decrypt the data without the secret key. And already, companies like Cloudflare[5] and AWS,[6] as well as open-source projects,[7,8] have begun to integrate PQC algorithms into their products.

But NIST's selection of these four algorithms does not fully resolve the issue of security after the quantum apocalypse; the selected algorithms cannot yet be put to the test against a real, appropriately powerful quantum computer. So, estimates of their protective capabilities are currently limited to mathematical proofs and simulation. Likewise, without a legacy of protection against both quantum and conventional threats at scale and in production, implementing PQC within a company's production environment today is a risky, and potentially costly, endeavor.

As adoption widens and the algorithms are tested in more and larger environments, these cost performance gaps will close, and production implementation will become more feasible for a wider range of applications and organizations. Only time will tell if NIST's currently selected algorithms offer the broad protection they promise and become widely adopted in the marketplace. The risk remains that these algorithms are found to be deficient or are otherwise unpopular, leaving open the possibility that one or more are soon replaced.

Should My Organization Adopt PQC Now?

Given the relatively low maturity of PQC technology, the uncertainty surrounding its long-term viability, and the current costs of implementation, most organizations will likely favor waiting for the ecosystem of PQC to mature further. This impulse, however, should be mediated by a careful analysis of each company's data, regulatory and customer requirements, risk posture, and current security practices, considering the "harvest now, decrypt later" attack pattern that quantum computing will facilitate. And the adoption of PQC does not need to be across all parts of your organization — in some cases, data that is at greater risk may need to be segmented and separately protected today, while other data types can be protected using business-as-usual methods.

To understand risks and help decide how to act, leaders should consider their data protection needs in relation to specific business and legal requirements, customer demands, and the overall risk posture of the business. From there, a decision can be made as to whether to pursue immediate adoption of PQC versus a wait-and-see approach.

DATA REQUIREMENTS

Conduct a review of the types of data you store — PI and PII, financial, credit cards, healthcare, FOUO/CUI, export-controlled — and any associated regulations, contractual requirements, or certifications that impose safeguarding and retention requirements on that data (e.g., HIPAA, FERPA, GLB, PCI-DSS, ITAR, EAR-99). If you have data today that must remain private for "more than 10 years," the risk you face could be enough to adopt PQC sooner rather than later.

CUSTOMER EXPECTATIONS

Your customers may have certain expectations for the privacy of their sensitive and personal information, such as archived emails, photographs, text messages, browsing histories, location data, and others. While customers may have limited

recourse in the case of a "decrypt later" event, remediation costs (e.g., breach notifications, identify theft insurance), reputational costs, and potential exposure to criminal or civil liabilities remain. If the potential impact of losing control of customer data in the future is high, you may also want to accelerate your plans to implement PQC for customer data.

OTHER REPUTATIONAL AND BUSINESS RISKS

Consider what potential other risks exist for a future breach of today's data. Is there potential for embarrassment and reputational harm from disclosure of internal communications? Would you face a competitive disadvantage stemming from the loss of trade secrets, research, and other confidential information? Are you storing digital keys that could be used to impersonate you, your company, or your products? If any of these are true, you may wish to enact quantum safeguards for these data types now.

What Else Should We Do Now?

Implementing quantum-secure encryption on your data is just one step in the process. Once you have assessed your risk factors and decided on an appropriate timeline for implementing PQC across your various IT systems, databases, and activities, consider other risks to your business that go beyond future-proofing your own encryption schemes. And even if you don't elect to adopt PQC soon, each of the suggestions below should be part of your near-term plans or business-as-usual operations.

PERIODICALLY RE-EVALUATE YOUR RISK

Your timeline and urgency for implementing PQC is predicated on the impact of loss, as well as the quantum apocalypse's presumed time horizon. Changes to either will impact your timeline, so you should periodically (we recommend quarterly) re-evaluate the risk factors and adjust your plans accordingly. In the meantime, stay alert for any changes to the nature of your data or your overall risk posture, updated legal or regulatory requirements, sudden and material advances in quantum computing development, or a reduction in the costs associated with adopting PQC. We recommend assigning a member of your team to monitor and present on the state of quantum computing as part of monthly or quarterly reporting.

MAINTAIN BEST-IN-CLASS, BUSINESS-AS-USUAL SECURITY PRACTICES

Prior to implementing PQC across your production environment, your data will be vulnerable to the threat of "harvest now, decrypt later" schemes. That's why it's imperative for you to prevent criminals from accessing the encrypted data today. This involves implementing and maintaining best-in-class measures to defend your systems and data so that it is never accessible or able to be exfiltrated.

If your business lacks a robust approach to information security, consider adopting a cybersecurity framework such as NIST's Cybersecurity Framework or ISO 27001 and a set of common security controls as a starting point. If your business already has a mature information security program, the most important thing will be to stay ahead of the threat: continue to build a culture of cyber safety, keep up to date with security best practices, and adjust as new technologies come online.

CHECK WITH SUPPLIERS

Regardless of your timeline for PQC adoption, you should check with suppliers to ensure that they have a plan to protect any data, systems, or applications they provide, support, develop, host, or manage on your

behalf — both against quantum and traditional threats. Implementing PQC on your own systems will be meaningless if attackers can still access your data or systems through a compromised and trusted supplier.

PUSH FOR REGULATORY AND LEGAL CLARITY

Much of the risk described here comes from the idea that you may have liability in the future due to negligence or carelessness today. Yes, perhaps a breach of fully and properly encrypted data today is a non-event now, but if it is later decrypted by quantum computers, will you suddenly become liable for past inaction on PQC? This will certainly be true in some domains where there is little tolerance for risk. In others, it is an unknown and perhaps will become a novel legal question at some point in the future. However, this does not have to be an unknown. We recommend that you work on two fronts to protect yourself from this risk. The first is to ensure that contracts and licenses are appropriately clear and specific on your liability in these cases. The second is to engage legislative leaders and advocacy groups to draft laws and frameworks to address the underlying issues and create certainty for businesses and the legal community.

UPDATE DISCLOSURES AND INSURANCE

You may not be able to prevent the quantum apocalypse from impacting you, but you can ensure that your response is ready now. Update disclosure notice language for your customers and clients to account for the possibility of future disclosure and ensure that they have access to appropriately long-lived remedies. If you've had a breach as recently as 2015, you may want to reach back out to affected parties to ensure that they're updated, too. And make sure that you have appropriate insurance against cyber threats that cover the threat of quantum computing, so that future incidents are properly covered.

FIND A PARTNER TO HELP YOU SORT OUT THE DETAILS

There will be many facets of the journey to and through the quantum apocalypse that involve considerable complexity and require organizational, process, and change management expertise. Make sure you have a trusted partner to help your business identify all the areas of your business that will need to change. Plan the transition so that you can focus on successful execution.

Fears and warnings about the quantum apocalypse are not new,[9] but as the size and sophistication of quantum computers continue to grow, so too does the threat. Regardless of your specific approach to cryptography in the quantum age, make sure you have a plan that considers the specific risks to your business. Manage your risk today even if that doesn't involve PQC. Finally, stay tuned for advances in quantum computing technology that may alter your approach. When the quantum apocalypse arrives, it is likely to be sudden and lead to considerable chaos. So, make sure your systems and processes are well ahead of the threat and well-positioned to manage any crises as they emerge. 🔑

Andrew Hardin
andrew.hardin@jabian.com

Sources:

1 *www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/*
2 *forbes.com/sites/arthurherman/2021/06/07/q-day-is-coming-sooner-than-we-think/?sh=45ed76f33f5d*
3 *csoonline.com/article/3643692/collect-today-decrypt-tomorrow-how-russia-and-china-are-preparing-for-quantum-computing.html*
4 *csrc.nist.gov/projects/post-quantum-cryptography*
5 *github.com/cloudflare/circl*
6 *aws.amazon.com/kms/*
7 *openquantumsafe.org/*
8 *github.com/PQClean/PQClean*
9 *arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/*