Quantum Security Alliance (QSA)

NIST Quantum Proof Algorithm Analysis

August 19, 2022

Authors:

Dr. Albert Carlson, QSA, Chair for Encryption & Entropy, Computer Science Dept., Austin Community College,
Orchid: 0000-0002-0087-6066

Dr. Keeper L. Sharkey, QSME, QSA, Chair for Quantum Applied Chemistry, ODE, L3C,
Orchid: 0000-0002-3767-6261

Editor Review:

Dr. Merrick S. Watchorn, DMIST, QIS, QSA Program Chair
Orchid: 0000-0003-2460-8689

Dr. Hans C. Mumm, QSA, Chair for Continuous Diagnostic and Monitoring, Victory Systems, LLC,
Reuters Researcher ID: B-8496-2013

Dr. Nancy W. Grady, QSA Chair for Quantum Artificial Intelligence and Machine Learning
Orchid: 0000-0003-2967-8221

Executive Summary

In July 2022, The National Institute of Standards and Technology (NIST) announced four finalists for standardizing Post-Quantum Cryptography (PQC) methods. The effort put forth aims to protect information through public-key cryptographic algorithms even with the advent and potential threat of quantum computer's (QCs) ability to crack the encryption key, which is thought to be possible due to the exponential computational space that current qubits supposedly offer. We explore the various types of Quantum Public Key Algorithms (QPA's) and include a discussion on the strengths and weaknesses of each finalist. Additionally, we present an explanation of the report on cracking a QPA finalist with a single traditional classic core CPU and the elapsed time calculation to break the algorithm. The six-year effort in the test and evaluation of the four finalists represents the efforts of numerous scientists and working groups to establish the emerging standards for quantum proofing the United States Government (USG).

The Quantum Security Alliance (QSA) was established in December 2018 and had been working rapidly to provide context to the emerging security landscape for Quantum Computing (QC). In the last several years of activity, the QSA has worked on numerous efforts, including aiding the Cloud Security Alliance (CSA), Quantum Tech Congress, and the National Defense University (NDU) in building a working knowledge-sharing model that includes the University of Maryland, University of Phoenix, and Purdue Global Online University. "Cybersecurity methods are riddled with new technologies such as Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), Operational Technologies (OT, IoT, SCADA, CPS, etc.), cloud computing, blockchain, and Quantum Information Systems (QIS)" [Watchorn, Bishop, Mumm & Brooks, 2022].

Since 2013, the United States and its Allies have endured a constant, sustained effort to reduce national security, resiliency, and confidence and undermine infrastructure found within Digital Warfare Strategies espoused by its enemies. This continuous strain has incurred a strategic financial, technical, and workforce debt not seen before in the cyber domain. Cloud computing enabled distributed computing at an economically affordable scale to commerce and the first integration of quantum and cloud with its success. When cyber adversaries have access to the power of quantum computing, our modern cryptographic systems based on public keys will not stand up to the test [NIST, 2021]. The White House led an effort to establish the National Quantum Initiative Act (NQIA), which became Public Law 115-368 in 2018, to accelerate American leadership in QIS, chemistry, and technology [NTSP, 2021]. This announcement was followed by the National Academies of Science, Engineering, and Medicine (NASEM) efforts to Identify Opportunities at the Interface of Chemistry and QIS [NASEM, 2022].

Keyword(s): Quantum; Quantum Computing; Quantum Chemistry; Quantum Public Key Algorithms; National Institute of Standards and Technology; USG; Computing; Security; Quantum Security Alliance; National Academies of Science, Engineering, and Medicine (NASEM) efforts to Identify Opportunities at the Interface of Chemistry; National Quantum Initiative Act; National Defense University; Post-Quantum Cryptography; Shannon Information Theory; Quantum Cybersecurity Awareness and Resiliency; Quantum Information Systems; Cloud; Cloud Computing; Hybrid Computing; High-Performance Computing; NP-Hardness; Encryption; Public Key Infrastructure; Q-Chem; Quantum Multi-Level Security; Polymorphic Encryption; Mathematics; Q-Labs, Sandbox AQ; Post-Quantum Environment

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

Background

Today's computing environment is generally categorized into two silos: classical computing and quantum computing. Both solve general use problems, but they do so using different hardware architectures and arrive at their answers differently. They both do the same mathematics and come to the same answers. This points to the critical point that mathematics remains the same in both computing environments; only the algorithm and manner of arriving at an answer change. Threat actors are actively stealing data to decrypt later (SNDL) once quantum computing capabilities are realized [Schwartz, 2022]. The National Security Agency (NSA) concluded that QC realization may not occur until at least 200,000,0000 qubits of processing power was capable; however, the release of the most recent QPA's has shown that in some respects, the SNDL quantum attack pattern does pose a national security threat today, vice in the perceived future. For example, the alleged NIST QPA cracking of the SIKE was first announced by Wouter Castryck & Thomas Decru at KU Leuven, and the attack was based on the "glue and split" theorem developed by Errist Kani as proposed in 1997 [Schwartz, 2022]. The use of a non-Quantum machine exposes the potential weakness of the SIKE approach, and members of the QSA began the analysis process.

For example, consider Shannon Information Theory (IT). In the mid-to-late 1940's and early 1950's Claude Shannon researched encryption [Shannon, 1949] and laid down what became the fundamentals of IT [Cover, 2005]. The study of IT laid down the mathematical foundations of information accumulation and how entropy [Garrett, 2004] is related to cryptography, and how entropy relates to both language redundancy (repetition) and unicity distance (the average amount of input data needed to distinguish the input unambiguously). These math concepts are valid no matter how the user arrives at a solution. However, some algorithms to do the math are not valid on classical and quantum computers because of the machine's architecture. Shor's algorithm [Shor, 1994] is one such algorithm that works on quantum machines but has no equivalent classical computing procedure. However, the use of Shor's algorithm should not be seen as breaking IT; but rather, it is a new heuristic algorithm and approach to solving some forms of cryptography. Other asymmetric-key trapdoor functions are still effective despite Shor's algorithm. Shannon theory and IT mathematics are still valid in the Post-Quantum Environment (PQE) as they are not based on an implementation but are pure math.

It is true that quantum computers are faster and allow some forms of math to be implemented more efficiently. However, Shor's algorithm only applies to asymmetric key PKE trapdoor problems based on variations of the discrete logarithm problem, prime and semi-prime factorization, and Euler's totient function [Mavroeidis, 2018]. Based on trapdoor functions that are hard in the classical computing architecture but vastly easier for a quantum architecture, quantum computing has shown that these functions are not a trapdoor for quantum systems. While PKE encryption systems available today are generally known to be susceptible to quantum computer architectures, symmetric key algorithms do not share the same problem. Quantum computers are generally faster than classical computers. Some speed improvements are gained by trying to break symmetric key encryption systems on quantum computers, but this speed/architecture advantage is not nearly as effective. The critical piece of research on symmetric algorithms is the result of Grover's algorithm, developed in 1996 by Lov Grover [Grover, 1996]. Grover's algorithm has shown that symmetric key algorithms must increase their key space by a factor of 2 because that

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

algorithm reduces the number of required access by a factor of $\frac{1}{\sqrt{2}}$. This means that symmetric key algorithms are still important and relevant in the PQE.

Because of the effect of Shor's algorithm eliminating the security present in PKE algorithms, governments have funded QC research. At the same time, it has been assumed that the use of symmetric algorithms was also totally broken. This is, however, not true. In addition, encryption efforts in the PQE have pivoted to Quantum Key Distribution (QKD) and entangled particle schemes. Some research experts feel these mechanisms render encryption moot, but this is similarly false. Because both asymmetric and symmetric algorithms remain valid, researchers have been searching for strong encryptions in both the classical and QC environments.

As a result of this research, two types of PKE encryption algorithms have been identified to date as "probably" being difficult to break in both computing environments. This is important as it is likely that the evolution of computing will result in a widely used computing platform that is a hybrid computer with both types of cores available in that computer for problem-solving. The reason for such a computer is that both types of approaches solve some problems far more efficiently than the other type will solve those problems. Encryption will have to survive both cores in order to be useful. The identified PKE encryption approaches identified in this research are both based on structured lattices and one of two forms of the Shortest Vector Problem (SVP) [Yasuda, 2021]. There are several different SVP problems. However, there are two versions of the problem used by finalists of the NIST QPA contest. One problem is that specific vectors are fitted in a multidimensional matrix. The other specific SVP problem is the Learning with Errors (LWE) approach [Regev, 2005].

The LWE problem [Regev, 2005] requires an attacker to determine the matrix based on a number of vectors selected from it. LWE has the added feature that it can be shown that the average amount of work required to find a solution is equal to the worst-case effort to find a solution. Both approaches are thought to be, and are presently, hard to solve. But, of course, this could change in the future in the same way that the CBC mode was thought to be hard until McGrew [McGrew, 2013] and Carlson [Carlson, 2015] separately developed the Collision attack. Because encryptions, even QPA's, are bijective and designed to be reversible, they are not totally random. This means that they will have a deterministic function based on its key. However, when there is a deterministic and limited key space, Shannon's theory indicates that there will be a unicity distance and attacks that can break the cipher [Shannon, 1949]. Present analysis on QPAs indicates, for instance, that an LWE-1024-sized cipher has the equivalent security of AES-256, which is a deterministic function.

The equivalence of security suggests that these ciphers should be seen as building blocks and used as a cipher library component. The polymorphic cipher engine is a new entrant into the security realm [Carlson, 2021]. Polymorphic engines are not single ciphers but instead use different ciphers for a short time ("shard") and then select a new cipher and key pair to inject entropy into encryption and make the cryptographic process secure [Carlson, 2022]. The result of the polymorphic process is that the constituent ciphers are made more secure than they would be if used by themselves. But what makes them more secure is that symmetric ciphers can also be added to the library to mix the cipher algorithms further. This mixing creates a framework, or "engine" that generates a series of encryptions for the shards that are much more random and secure than using any single cipher.

We discuss the concept of shards in a white paper published in August 2022 called "Standard Password Practices for Organizations: Relative Theory and Recommendations" [Carlson, 2022, B]. The engine can use any cipher as part of the library of available ciphers. Because the keys and ciphers are chosen randomly and do not rely on any preceding information, they are orthogonal to each other. Each encryption problem is independent of any shard that precedes or follows. The same behavior also means that since they are orthogonal, the shards may be processed in parallel due to a lack of dependencies. As a result of this sharding of the message, overhead and latency are reduced. Finally, the message can be encrypted faster than other non-trivial ciphers. The greater the number of threads/cores/GPUs in the machine, the faster the encryption/decryption. Sharding is also scalable, allowing the shard to be reduced in size as computer speed increases with decreasing feature size. This makes polymorphic ciphers future-proof, as well.

QPA Discussion

NIST has recently been involved in selecting encryption and hashing algorithms to replace those PKE encryptions and PKI components that are known to be vulnerable to the PQE and application of Shor's algorithm. Several hundred algorithms were submitted, and of these, NIST has recommended several as finalists in the competition for standardization [NIST, 2022]. However, this process has not been without some controversy. For instance, one of the finalists in the encryption category was broken after initial testing by an attack that takes less than an hour to run on a classical computer [HackerNews, 2022]. However, this revelation does not give confidence in the testing regimen applied to the submissions. This announcement removed Supersingular Isogeny Key Encapsulation (SIKE) from consideration for further use.

All of the finalists have what is called a "hardness measure" in the studied literature. The hardness measure is, in effect, the unicity distance measure of Shannon's Theory analysis and should be seen to compare resistance to analysis and the maximum size of the message (or shard) for application in encryption or signature. NIST has also taken pains to try and protect against side-channel attacks (SCA). SCAs have been used to break ciphers using hardware hacks, time measurements, and a wide variety of tactics to break encryptions without resorting to directly reversing the trapdoor function. Unfortunately, these attacks are often more efficient and quicker than mathematical attacks.

The remaining NIST's fourth round of competition algorithms suggested for use in PKE/PKI applications in the PQE by NIST are CRYSTALS – Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. We explore the pros and cons of each in the following tables:

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

First, we discuss an ***Encryption*** method; CRYSTALS – Kyber.

CRYSTALS is an acronym for "CRYptographic Suite for Algebraic Lattices," and the Kyber tool makes use of the IND-CCA2-secure key encapsulation mechanism (KEM). It is an NP-hard algorithm named after the mythical kyber crystal used to power light sabers in the Star Wars universe. One of the goals for Kyber is to maintain about a 4:1 ratio between Kyber and AES. Performance data is available on the Kyber website [PQCrystals, 2020].

Algorithm	Pros	Cons	Foundation Technology
CRYSTALS – Kyber	Small keys Easy key exchange Fast	Key size to security ratio (The 1024-bit key version has about the same security as AES 256)	Structured Lattices - LWE

Next, we discuss ***Digital Signature Algorithms:*** CRYSTALS-Dilithium, FALCON, and SPHINCS+

Their foundation problem, pros, and cons are listed in the table below.

Algorithm	Pros	Cons	Foundation Technology
CRYSTALS-Dilithium	Computational Efficiency, Key size of 1196 – 5892 bits, Many memory/speed trade-offs are possible, Easier to detect bugs, Faster key generation, Uses less memory	Same technology algorithm as FALCON	Structured Lattices – SIS and LWE modules
FALCON	High Efficiency	Same technology algorithm as Dilithium, More susceptible to implementation errors, Harder to mask	Structured Lattices - SIS and LWE modules
SPHINCS+	Follows known hard algorithms	Only for smaller signatures, large, slow speed	Hashes

A comparison of the Dilithium and FALCON was published by NIST [NISTDilithium, 2022]. This site gives algorithm specifics and performance measurements.

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

SPHINCS+ was presented at Eurocrypt 2015 and is the product of a team of developers. The main goal of the effort was to reduce signature size using a stateless algorithm [Schwabe, 2022]. It is primarily based on hash algorithms and is known to be both resource intensive (large) and slower than either Dilithium and FALCON. It is envisioned to have niche applicability for those reasons; the code for SPHINCS+ is linked to the developing organization web site.

Conclusion

There are many similarities in the development of classical and quantum computers. There are similarities and some glaring differences between the architecture and capabilities of both types of computers. These differences do not, however, change mathematics and the theory built on math. The same mathematics applies, especially in Information Technology (IT). No difference in the instantiation of the computing machine can, or will, change the base theory. Trapdoor functions upon which encryption is built will change and are affected by the architecture and heuristic programming techniques used by each technology. Some problems are best solved with classical computers and some with quantum computers. This makes it likely that hybrid computing environments with both capabilities will eventually become the norm. Therefore, security must be strong for both types of computers. This was graphically illustrated by a classical computer's recent break of SIKE encryption [NIST, 2022] in under an hour.

NIST recently released its recommendations for encryption and signature algorithms. However, it is too early to say if the QPAs are really strong. Testing continues to verify the efficacy of the algorithms, and many attacks and approaches have yet to be used on those algorithms. To have a finalist broken so easily after reaching the final recommendation level does not give users confidence in the current vetting process. Instead, the base technology of the QPA algorithms gives hints that they may be susceptible to newer attacks, such as isomorphic keys space reduction.

To be clear, all ciphers are breakable. Brute force attacks are always successful. If they were not, there would be no way to decrypt messages. The question is whether known heuristic attacks can be successful against the finalists. In the future, new attacks will probably be developed to be relevant and effective against these QPAs. Such actions have historically taken place and are responsible for the evolution of ever more complex and effective ciphers. Such research also benefits the field by pointing out essential principles and practices in both breaking ciphers and protecting the underlying information. For example, one of the main principles in cryptography was articulated by Shannon. That is to inject entropy to lengthen the unicity distance. Perhaps the question in this situation should be, why rely on a single cipher? PKE was based on the question, 'if one password is good, then it makes sense that two passwords make for a stronger encryption modality.' In that vein, if one cipher is good, aren't more than one better? We recommend that additional robust algorithms be identified and added to libraries that can be shared and used polymorphically. Using polymorphic engines increases security by irregularly but frequently injecting entropy and breaking the more significant problem into smaller problems.

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

Moreover, the information does not accumulate sufficiently to allow for decryption. It can also speed up the encryption/decryption process by taking advantage of the orthogonal nature of the problems. This is not the whole answer. Instead, users should employ the best new quantum technologies, such as quantum key distribution (QKD) and particle entanglement, to increase security. This use highlights that QKD and entanglement are not complete answers to security alone.

At this point, the QPAs appear to be founded on strong algorithms. However, this does not mean that they are infinitely strong. For example, Shannon's IT and cryptography theory says that if a sufficient corpus of encrypted data is available, then decryption is possible. The answer to security is to leverage these strong ciphers into an even more robust polymorphic encryption system.

Much is being discussed in the way of hybrid-computing systems; however, little is being discussed on how to secure these hybrid systems, and even less is being discussed about securing end-to-end quantum computers. This approach allows QC to be introduced into the national security arena with cyber security risks, supply chain issues, an increase in performance, and an increase in natural language abilities. The threat of unchecked technology and the ability to weaponize QC continue to evolve. Quantum solid-state memory advancements have offered more sophisticated capabilities with cost-effective designs resulting in a reduced entry-level for consumers, businesses, enemy states, and terrorist organizations. As a result, 'QC's reduced barrier to entry is now a national security risk.

These issues are being discussed by the Congressional Research Service (CRS) as QC "could hold significant implications for the future of military sensing, encryption, and communications, as well as for congressional oversight, authorizations, and appropriations" [Gallo, 2021]. The QSA proposes using these types of external validators to build a hybrid model to analyze and evaluate the required control paradigms at each stage of dynamic quantum circuits (Q-CI). The key to this entire discussion on weaponization comes down to security. "As information becomes the world's most valuable commodity, nations' economic, political, and military fate will depend on the strength of ciphers…demolish(ing) the concept of national security. A quantum computer would jeopardize the stability of the world" [Bacon, 2006]. Current QISs are not optimized for cybersecurity design practices, let alone optimized for hybrid computing as the flow of information moves from classical computers (including AI and 5G systems) to quantum computers and back again [Carlson, Mumm, Sharkey, Watchorn, 2022]. The QSA research group continues to explore the impacts of QC and its pros and cons to help grow Quantum Cybersecurity Awareness and Resiliency (QCAR) into future standards, operational guidelines, and legislative efforts.

Point of Contact: Dr. Merrick S. Watchorn, DMIST at ceo@quantumsecurityalliance.org

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

References

[QL, 2022] Quintessence Labs, "Quintessence Labs Sits at the Intersection of Quantum & Cyber," https://www.quintessencelabs.com/products#qrand-200

[Bacon, 2006]. Quantum Computing Shor's Algorithm. In: Department of Computer Science & Engineering, University of Washington.

[Carlson, 2015] Albert Carlson, Patrick Doherty, Isaiah Eichen, and James Gall, "Breaking CBC or Randomness Never Was Happiness," *Defcon 23*, Las Vegas, NV, 2015

[Carlson, 2021] Albert Carlson, Indira K. Dutta, Bhaskar Ghosh, and Michael Totaro, "Modeling Polymorphic Ciphers," *Sixth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2021

[Carlson, 2022] Albert H. Carlson, Sai Ranganath Mikkilineni, Michael Totaro, Robert Hiromoto, and Richard B. Wells, "An Introduction to Local Entropy and Local Unicity," *International Symposium on Networks, Computers, and Communications, ISNCC 2022*, 2022

[Carlson, 2022, B] Albert H. Carlson, "Standard Password Practices for Organizations: Relative Theory and Recommendations," LinkedIn: https://www.linkedin.com/posts/quantum-security-alliance_qsa-password-practices-for-organizations-activity-6960699759506407424-nAHa?utm_source=linkedin_share&utm_medium=member_desktop_web

[Carlson, Mumm, Sharkey, Watchorn, 2022] Albert H. Carlson, Hans C. Mumm, Keeper L. Sharkey, Merrick S. Watchorn, "Quantum Chemistry for Detecting Cyber Security Threats", LinkedIn: https://www.linkedin.com/posts/quantum-security-alliance_q-chem-for-detecting-cybersecurity-threats-activity-6951226103449489408-jPMu?utm_source=linkedin_share&utm_medium=member_desktop_web

[Cover, 2005] Thomas Cover and Joy Thomas, Elements of Information Theory 2nd ed., John Wiley & Sons, Inc: New York, 2005

[Gallo, 2021]. Defense Primer: Under Secretary of Defense for Research and Engineering. Retrieved from Washington DC: https://apps.dtic.mil/sti/citations/AD1125422

[Garrett, 2004] Paul Garrett, The Mathematics of Coding Theory, Pearson/Prentice Hall: Upper Saddle River, NJ, 2004

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

[Grover, 1996] Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)*, Association for Computing Machinery: Philadelphia, Pennsylvania, USA, pp. 212–219, 1996

[HackerNews, 2022] Ravie Lakshmanan, "Single-Core CPU Cracked Post-Quantum Encryption Candidate Algorithm in Just an Hour," https://thehackernews.com/2022/08/single-core-cpu-cracked-post-quantum.html, August 3, 2022

[Mavroeidis, 2018] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang, The Impact of Quantum Computing on Present Cryptography, *International Journal of Advanced Computer Science and Applications (IJACSA)*, v. 9 no. 3, pp. 405-414, March 2018

[McGrew, 2013] David McGrew, "Impossible Plaintext Cryptanalysis and Probable-Plaintext Collision Attacks of 64-bit Block Cipher Modes," *Proceedings of the Fast Software Encryption Workshop*, 2013

[NASEM, 2021]. "Identifying Opportunities at the interface of chemistry and quantum information science," the National Academies, 2021. Retrieved from www.nationalacademies.org/en/our-work/identifying-opportunities-at-the-interface-of-chemistry-and quantum-information-science

[NIST, 2021]. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography

[NIST, 2022] NIST, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms, July 5, 2022

[NISTDilithium, 2022] Shi Bai, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lybashevsky, Peter Schwabe, Gregor, Seiler, and Damien Seiler, "CRYSTALS Dilithium," Retrieved August 15, 2022, https://csrc.nist.gov/CSRC/media/Presentations/crystals-dilithium-round-3-presentation/images-media/session-1-crystals-dilithium-lyubashevsky.pdf[NTSP, 2021]

[PQCrystals, 2020] Peter Schwabe, "CRYSTALS Cryptographic Suite for Algebraic Lattices," https://pq-crystals.org/kyber/, Last updated December 23, 2020

[Regev, 2005] Oded Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Proceedings of the Thirty- Seventy Annual ACM Symposium on Theory of Computing (STOC '05)*, Association for Computing Machinery: Baltimore, Maryland, USA 2005

[Schwabe, 2022] Peter Schwabe, “SPHINCS+,” 18 Jul 2022, http://sphincs.org/

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.

[Shannon, 1949] Claude E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, v. 28, pp. 656 – 715, 1949

[Shor, 1994] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994

[Schwarts, J., 2022]. Threat Actors Are Stealing Data Now to Decrypt When Quantum Computing Comes. https://www.darkreading.com/edge-articles/threat-actors-are-stealing-data-now-to-decrypt-when-quantum-computing-comes

[USG Congress, 2018]. National Quantum Initiative Act, H.R. 6227. https://www.congress.gov/bill/115th-congress/house-bill/6227

[Watchorn, Bishop, Mumm & Brooks, 2022]. Cybersecurity Legal Elasticity Antecedent Resilience (CLEAR) System. Quantum Security Alliance (QSA).

[Yasuda, 2021] Masaya Yasuda, A Survey of Solving SVP Algorithms and Recent Strategies for Solving the SVP Challenge, *International Symposium on Mathematics, Quantum Theory, and Cryptography*, pp. 189-207, 2021

Other resources:

https://info.quintessencelabs.com/hubfs/QLabs-qOptica-QKD-product-sheet-2.pdf

https://info.quintessencelabs.com/hubfs/QLabs-qStream-product-sheet.pdf

https://github.com/pq-crystals/dilithium

https://github.com/microsoft/PQCrypto-LWEKE

All rights reserved. All content on this document is protected by Quantum Security Alliance (QSA) copyrights and other protective laws.